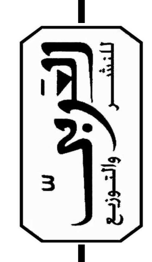

دراسات في
الإعلام
الإرهاب
والجريمة الإلكترونية
د. غادة نصار
العربي للنشر والتوزيع

الإرهاب والجريمة الإلكترونية
د. غادة نصار

الطبعةالأولى: يوليو**2017**

رقم الإيداع: 2017 / 11268
الترقيم الدولي: 978977319 3485
الغلاف: خالد شريف



60 شارع القصر العيني - 11451 - القاهرة
ت 27921943 – 27954529 فاكس 27947566
www.alarabipublishing.com.eg

بطاقة فهرسة

نصار، غادة
الإرهاب والجريمة الإلكترونية، القاهرة: العربي للنشر والتوزيع، 2017
ص؛ سم.
تدمك: 9789773193485
1– الجرائم الحاسوبيه 2- الإرهاب
أ – العنوان 346.168

الإرهاب والجريمة الإلكترونية

د. غادة نصار



مقدمة

لقد غزت التطورات التكنولوجية الحديثة مجتمعاتنا فى شتى مجالات الحياة. خاصة فى مجال الإعلام وهو ماسهل نقل المعلومة من مكان إلى أخر. فبفضل هذه التكنولوجيا أصبح العالم قرية صغيرة مفتوحة، يمكن من خلالها العبور إلى عوالم أخرى لم نكن لنصل إليها قط دون الوسائل التكنولوجية.

فالانترنت على سبيل المثال أصبح وسيلة لإكتساب أصدقاء جدد بغض النظر عن بعد المسافة، وكذلك الانتقال السريع للمعلومات، والتعرف على أخبار العالم وحتى أنه أصبح وسيلة للترويج للأفكار والمنتجات، ولكن كما لهذه الوسائل التكنولوجية فوائد جمة وفرت على البشرية الكثير من الوقت والجهد والنفقات.

إلا أنه تولد عنها مخاطر كبيرة قد تهدد أمن وكيان المجتمعات، والجريمة الإلكترونية أو الجرائم التى ترتكب من خلال الحاسب والإنترنت أحد هذه المخاطر، وما يجب الإشارة إليه أن هذه الجرائم توجد فى المجتمع العربى والمصرى وهى كالجرائم التقليدية لها مرتكبيها وضحاياها، إلا أنها قد تكون أخطر من الجرائم المتعارف عليها لأنه يتم ارتكابها عبر زر الكمبيوتر وهو ما سهل ارتكابها وجعل من الصعب رصد الجانى فيها وتتبعه والقبض عليه.

لذلك يجب على وسائل الإعلام المصرية والعربية توعية الشباب من مخاطر هذه الجريمة خاصة وأن الشباب أكثر الفئات المتعاملة مع الشبكة العنكبوتية، ومن ثم يكون أكثر الفئات تضررا من هذه الجريمة وأكثرها ارتكابا لها. فالجريمة الإلكترونية أحد الضرائب التى يدفعها الكثير من جراء التكنولوجيا الحديثة التى اجتاحت العالم بأثره؛ لأن التكنولوجيا مثلما اتاحت لنا الإنفتاح على العالم بمجرد الضغط على زر الحاسب، أوقعت بنا فى براثن الكثير منالجرائم الإلكترونية.

ولعل أخطر هذه الجرائم الإرهاب الإلكترونى الذى أصبح ظاهرة سهلت تجنيد وتدريب الشباب ولا سيما العربى واللعب فى أفكارهم ومعتقداتهم للتأثير عليهم، وتشجيعهم على القتل والتخريب فى مجتمعاتهم أو مجتمعات الغير تحت مظلة خادعة تسمى خدمة الدين الإسلامى.

والاسلام منهم براء. لذلك يهدف هذا الكتاب إلقاء الضوء على الجريمة الإلكترونية وأسبابها ووسائلها وكيفية ارتكابها وأشكالها المختلفة التى يحتل الإرهاب الإلكترونى أحد أشكالها وأخطرها.

الفصل الأول

الجريمة الإلكترونية

ماهيتها وأسبابها وطرق مكافحتها

أولاً: الجريمة الإلكترونية.

ثانياً: تصنيف الجرائم الإلكترونية

ثالثاً: أشكال الجرائم الإلكترونية.

رابعاً: خصائص الجريمة الإلكترونية.

خامساً: أضرار الجريمة الإلكترونية.

سادساً: أسباب زيادة الجرائم الإلكترونية فى مصر والوطن العربى.

سابعاً: ماهية المجرم الإلكترونى.

ثامناً: خصائص المجرم الإلكترونى.

تاسعاً: فئات المجرم الإلكترونى.

عاشراً: دوافع مرتكب الجريمة الإلكترونية.

حادى عشر: المعوقات التى تمنع توقيع العقاب على مرتكبى جرائم الإنترنت.

ثانى عشر:ضحايا الجرائم الإلكترونية.

ثالث عشر: أساليب مكافحة الجرائم الإلكترونية.

رابع عشر: سبل الأمان والحماية على الإنترنت.

دور التطورات المعاصرة فى ظهور الإنترنت.

إن التقدم فى تكنولوجيا المعلومات والإتصالات يعد أحد الأسباب وراء حدوث عملية العولمة. على الرغم من المزايا والمنافع الإيجابية المترتبة على هذه العولمة وثورة المجتمع الإلكترونى، إلا أنها ساعدت على ظهور وتعزيز أنواع جديدة من الجرائم ومنها على سبيل المثال جرائم غسيل الأموال وتهريب المخدرات، وإختراق قطاع الأعمال، الفساد، ورشوة الموظفين، والتدليس والغش، والإتجار غير المشروع فى الأسلحة[1].

ولكن ما نود الإشارة إلية أن الإنترنت مثله مثل غيرة من التطورات التكنولوجية له إيجابيات وسلبيات لذلك سنقوم بإلقاء الضوء عليها لعلنا نستطيع الإستفادة من هذه الإيجابيات وتجنب السلبيات.

العالم قبل ظهور الجريمة الإلكترونية.

قبل ظهور الإنترنت وجرائمه كانت توجد الأفعال الإجرامية، وكانت هذه الأفعال تشمل القتل والسرقة والنصب والتزوير وغيرها من الجرائم، فالشر قائم بيد ان الإنترنت ساعد على سهولة إرتكاب هذة الجرائم، فتقنيات الكمبيوتر سهلت إرتكاب الجرائم ففضاء المعلومات ليس له مبادىء أخلاقية عامة، فحدود السلوك المقبول أو حتى السلوك الأخلاقى فى فضاء المعلومات ليست واضحة، فضيف الكمبيوتر يمكنه الوصول إلى بعض المعلومات وعدم الوصول إلى البعض الأخر، بينما فى الإنترنت يمكن الوصول للمعلومات وقراءة البريد الإلكترونى للشخص بسهولة[2]، لذلك فوجود الانترنت أدى إلى تطور الجرائم التقليدية واستحداث جرائم جديدة. ومن العوامل التى ساعدت أيضا على ظهور الجرائم المستحدثة التغيرات فى البنية الأجتماعية والأقتصادية للمجتمعات الحالية، فمن الناحية الأجتماعية جاء تغير منظومة الأعراف والقيم الأجتماعية وتحولها من المحلية إلى العالمية ليولد سلوكيات جديدة منحرفة ومجرمة

1- أمير فرج يوسف: **"الجرائم المعلوماتية على شبكة الإنترنت"**، (الأسكندرية: دار المطبوعات الجامعية، 2008) ص.
2- السيد عتيق: "جرائم الانترنت" (القاهره: دار النهضه العربيه،2000) ص3.

لأنها خارج سياق القانون الوطنى، ومن الناحية الأقتصادية فإن عولمة المال والأقتصاد الناجمة عن زيادة الترابط الألكترونى والأعتمادية المتزايدة على التقنية والأتصالات فى تسيير الأعمال الأقتصادية وما نجم عن ذلك من مؤسسات وشركات متعددة الجنسيات وشركات عابرة للحدود الوطنية.

قد أسهمت فى بذور جرائم إقتصادية مستحدثة، ومرد ذلك هو تحول البنية الأجتماعية والأقتصادية إلى عالمية وإلى معلوماتية وألكترونية، وظهرت مسميات جديدة لمثل هذه الأبنية مثل الطريق السريع للمعلومات أو الأنترنت والبناء التحتى المعلوماتى العالمى، فالنادى التحتى المعلوماتى الألكترونى. ولم بعد كل ذلك وطنياً بل عالمياً مما أفرز جرائم مستحدثة ووضع ضغوطاً نحو عولمة القانون والأمن ومن أهم أنواع الجرائم المستحدثة لجرائم الإلكترونية[1].

1- محمد محمد الألفى : جرائم الإنترنت كأحد الجرائم المستحدثة بحث منشور على الأنترنت بتاريخ 2008/1/30 الساعة 1 ظهرا moelalfy@yahoo.com

أولاً: الجريمة الإلكترونية.

لقد اختلف الكثير من الكتاب حول تحديد شكل وتعريف الجريمة الإلكترونية ومن خلال الإطلاع على الكثير من المؤلفات لاحظت الباحثة الخلط الشديد بين كل من الجريمة الإلكترونية والمعلوماتية وجرائم الحاسوب و جرائم الإنترنت.

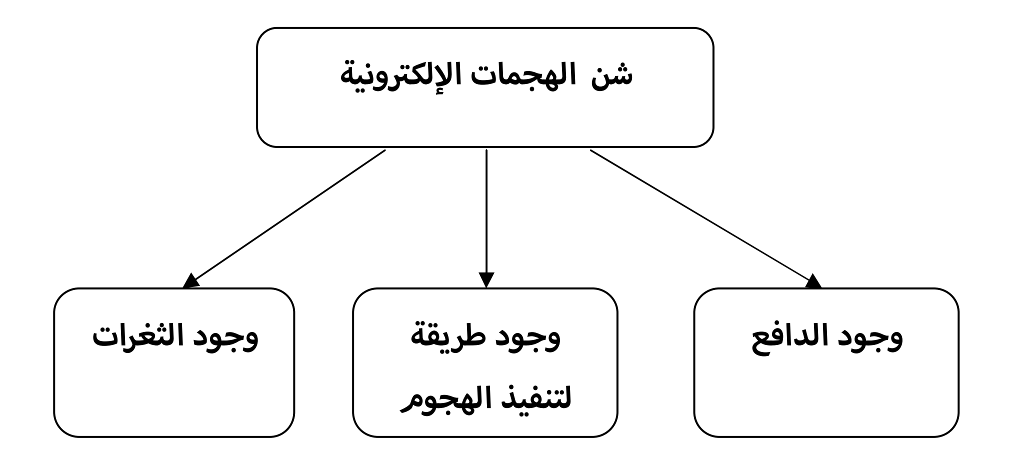
ويتضح هذا الخلط جليا عندما نرى بعض المؤلفات تتعامل مع الجرائم الإلكترونية وجرائم الإنترنت على انهما مفهوم واحد، بينما نجد من يتعامل مع جرائم الكمبيوتر والجرائم المعلوماتيه على أنهما مفهوم او مصطلح واحد، وهناك من يفرق بينهما فى المسمى.

ولكن من الملاحظ ان أشكال الجريمة بهم جميعا واحدة لذلك ووفقا للتعريف الإجرائى للدراسة فإن الجريمة الإلكترونية تشمل جميع أنواع الجرائم التى تتم من خلال أو بواسطة الحاسب الألى منفردا أو متصلا بالإنترنت. **وذلك:**

1- لتوافر مراجع ومؤلفات تسلم بهذا الأمر.

2- لحصر جميع الجرائم التى تتم بواسطة الكمبيوتر والإنترنت.

وقبل الاسترسال فى الحديث عن الجريمة الإلكترونية لابد من الاشارة إلى أن شن الهجمات الإلكترونية **يتطلب وجود ثلاثة عناصر.**



أ- وجود الدافع.

إن من يهاجم أى نظام معلوماتى لابد أن هناك ما يدفعه لذلك قد يكون الدافع رغبة فى الانتقام من الجهة المستهدفه أو الحصول على المال أو الاستئثار بأكبر قدر من الذبائن كما هو الحال بين الشركات المتنافسة.

ب- وجود طريقة لتنفيذ الهجوم.

من البديهى أن المهاجم لن يتمكن من شن هجوم ناجح مالم يكن لديه تصور وخطة واضحة لطريقة هجوم تحقق الغرض وهذا هو الفرق بين المهاجمين المحترفين وغير المحترفين ولصد هذه الهجمات أو تخفيف أضرارها يجب علينا معرفة طرق الهجوم وخططه ومتطلبات نجاح التنفيذ.

ج- وجود الثغرات.

والثغرة (Vulnerability) فى هذا السياق مصطلح يقصد به وجود نقطة ضعف فى تصميم أو تهيئة البرمجيات أو قواعد التخزين ونقاط الضعف هذه هى التى يتسلل المهاجم من خلالها لإحداث الدمار الذى يريده[1].

وبإختلاف هذه العناصر الثلاث يختلف أنواع وتصنيفات الجرائم الإلكترونية.

1- خالد بن سليمان الغثر، محمد بن إبراهيم السويل: "**أمن المعلومات بلغة ميسرة**"، (الرياض: ب.د، 2009) ص25 ،24.

ثانياً: تصنيف الجرائم الإلكترونية[1].

م	جرائم عامة	جرائم مادية	جرائم اقتصادية	جرائم ضد الأفراد
1	أخطاء الأداء المتعمد	السرقة	النصب والإحتيال	القذف والتشهير
2	اغفال الواجب	التدمير والإتلاف	الاختلاس	تسهيل الدعارة
3	التجاهل	تزييف المستندات	الرشوة	إنتهاك الخصوصية
4	التهور والطيش	التعدى على الممتلكات	الإبتزاز	الإهانة
5	التأمر والتواطؤ	السطو الليلى	التهديد	التحرش الجنسى
6	-	التهريب	إنتهاك الاسرار الاقتصادية	الخطف
7	-	انتحال الشخصية	التزييف والتزوير	القتل
8	-	قرصنة البرامج	-	الانتحار
9	-	التجسس العسكرى	-	-
10	-	التجسس الصناعى	-	-
11	-	التجسس الاقتصادى	-	-

1- طاهر داود: **"جرائم نظم المعلومات"**، (الرياض : ب د، 2000) ص38.

ثالثاً: أشكال الجرائم الإلكترونية.

تعتبر شبكة الإنترنت سلاحا ذو حدين، فمن ناحية تؤدى خدمات جليلة وعظيمة للدول والمنشأت التجارية والصناعية والعلمية والمستهلكين فى جميع أنحاء العالم، وأصبح بإمكان أى دولة أو جامعة أو شركة أو فرد أن ينشىء لنفسه موقعا على هذه الشبكة، وبإمكان أى شخص الوصول إلى موقعها بيسر وسهولة.

هذا التطور السريع فى هذه الشبكة، وتصميم استخدامها على مستوى سكان العالم بصرف النظر عن أوطانهم أو عقائدهم أو اتجاهاتهم الفكرية جعل البشر فى هذا الكون يتجه إلى تكوين مجتمع عالمى واحد بإستطاعة أى فرد أن يدخل إلى هذه الشبكة، ويتجول فى العالم من غير حدود ولا قيود ولا رقيب.

هذا التطور الكبير المتسارع لشبكة الإنترنت صاحب ظهور جرائم مستحدثة ما كانت لتعرف لولا ظهور هذه الشبكة، وهكذا أصبحت شبكة الإنترنت موضعا لكثير من الجرائم، وساعد على ذلك أمور منها:

أ- أن هذه الشبكة لا تخضع لهيئة أو حكومة معينة، ولا توجد إدارة مركزية لها، كما لا تخضع لأى تنظيم أو اتفاق دولى فى الغالب.

ب- عدم الإتفاق بين الدول على التعريف القانونى للجريمة المتعلقة بالإنترنت.

ج- نقص الخبرة لدى الشرطة وجهات الإدعاء والقضاء فى هذا المجال لتحديد عناصر الجريمة وأكانها وجمع المعلومات والأدلة منها.

د- غياب مفهوم متفق عليه بين الدول فى تحديد ما العمل الذى يمثل جريمة وللعمل الذى لايمثل جريمة من خلال شبكة الإنترنت.

هـ- أن السمة البارزة للجرائم الإلكترونية أنها غير أقلية بل هى عابرة للحدود فقد يكون المجرم فى قارة وتقع الجريمة فى قارة أخرى[1].

1- https://ar.wikipedia.org/wiki

وفيما يلى شرح مفصل لأشكال الجرائم الإلكترونية:

أ- الجرائم الجنسية والإباحية وغير الأخلاقية.

يوجد مواقع على شبكة الإنترنت تحرض على ممارسة الجنس سواء على الكبار او الأطفال وتقوم هذه المواقع بنشر صور جنسية أكثر تخصصية، فمنها ما هو متخصص فى أفلام الفيديو ومنها ما هو متخصص فى الصور وكثير منها متخصص فى برامج المحادثة.

وهذه المواقع تجد اقبالا كبيرا على زيارتها وتصفح محتوياتها وقد تم حصر المواقع الإباحية العربية دون الأجنبية على شبكة الإنترنت فوجد أنها تصل إلى 71 موقع[1].

ب- قرصنة البرامج عبر شبكة المعلومات.

تعتبر قرصنة البرامج من الجرائم التى ارتبطت بنشأة الحاسبات الألية بصفة عامة، إلا أن ظهور شبكات المعلومات قد ساعد على نحو كبير فى زيادة حجم هذه الجريمة لما وفرته هذه الشبكات من مجال خصب لارتكابها، فالطبيعة المفتوحة لشبكات المعلومات بالإضافة إلى ارتفاع قيمة هذه البرامج فى الأسواق وسهولة إعادة نسخها فى ثوان معدودة، ووما توفره هذه الشبكات أيضا من مجال خصب لتسويق هذه البرامج المنسوخة قد أغرى قراصنة البرامج لمارسة أعمالهم داخل الشبكة[2].

1- عمرو عيسى الفقى: "**الجرائم المعلوماتية وجرائم الحاسب الألى والإنترنت فى مصر والدول العربية**"، (القاهرة: المكتب الجامعى الحديث، ب ت) ص96،97.

2- نائلة عادل محمد فريد قورة: "**جرائم الحاسب الاقتصادية**"، مرجع سابق ص31،32.

وما يجدر الإشارة إليه أن عدد عمليات الإختراق التى يقوم بها الهاكرز 75 عملية إختراق على سبيل المثال وليس الحصر:

1- عمليات التثبيت الإفتراضية.

2- كلمات المرور غير الأمنة.

3- عدم وجود نسخ احتياطية جيدة داخل النظام أو غياب تلك النسخ على الإطلاق.

4- الزيادة المفرطة فى اعداد منافذ الاتصال المفتوحة.

5- الأساليب غير الجيدة المستخدمة فى تنقيح حزم البيانات أو غيابها على الاطلاق.

6- عمليات التسجيل غير الفعالة أو غيابها على الإطلاق.

7- تجاوز سعة الذاكرة المؤقتة.

8- سرد الأدلة وتنفيذ الملفات المشتملة عليها وحدة الخدمة الخاصة بالويب[1].

1- جون كيريللو: **"موسوعة الهاكرز"**، ط2 (القاهرة: دار الفاروق للنشر والتوزيع،2007) ص 600، 590.

وهناك عدة طرق لمواجة تسلل الهاكرز:

1- قامت بعض الشركات الكبرى بتعيين العديد من الهاكرز كمتخصصى أمن، بالإضافة إلى ذلك اتحد بعض الهاكرز وقامت بتكوين شركات للإستشارات الأمنية.

- يمكن تثبيت أداة (Zonealarm) المجانية والقوية والمتميزة، وتقوم هذه الأداة الشخصية بإخفاء جهازك فى مخبأ سرى.

2- يمكن اجراء اختبارات (Shields up) حيث يمكنك قراءة الصفحات المعروضة على موقع (Steve Gibson) حيث تعرض هذه الصفحات كيفية منع أى تسلل وفحص خارجى، ووقف تشغيل المنافذ وغيرها من الحلول[1].

1- ريتشارد مانسفيلد، ترجمة خالد العامرى: **"حيل وأساليب الهاكرز وطرق الوقاية منها"**، ط2 (القاهرة: دار الفاروق للنشر والتوزيع، 2006) ص31،32.

جـ- إتلاف المعلومات.

يتحقق اتلاف المعلومات عن طريق ضرب وحدات تشغيل المعلومات بأدوات ثقيلة، واستعمال الحريق بها، أو تفجيرها بشحنات ناسفة، أو باستخدام قنبلة غاز قارض، أو مواد ملتهبة، أو العبث بمفاتيح التشغيل.

ذلك يتحقق الإتلاف عن طريق محو بطاقة التعريف بماهية المعلومات المختزنة، أو بمسح البرنامج أو اخفاء بعض البطاقات، أو خربشة شريط إلقاء طفى السجائر على الإسطوانات، كذلك يمكن افساد المعلومات المختزنة مغناطيسيا بإخضاعها لقوى مغناطيسية متلفة[1].

وفى الغالب تأخذ جرائم اتلاف المعلومات أحدى الصورتين:

1- استبدال المعلومات.

استبدال المعلومات من الأمور السهلة أيضا فى جرائم اتلاف، استبدال رقم بأخر وإحلال رقم محل أخر، وهو نوع من جرائم التزوير على درجة كبيرة من الخطورة لأنه فى حالة نجاحه يستمر فترة طويلة من الزمن ويتولد عنه مكاسب كبيرة.

2- محو المعلومات[2].

ونظرا لما تتعرض له المعلومات من جرائم سواء بالإستبدال او المحو أو حتى السرقة فإن بعض الدول تضع قيودا على تداول المعلومات وهذه الدول تطلب فى حالة انتقال هذه المعلومات إلى دول أخرى أن تلتزم هذه الدول بنفس مستوى الحماية المفروض على هذه المعلومات[3].

1- محمد حسام محمود لطفى: **"الحماية القانونية لبرامج الحاسب الإلكترونى"**، (القاهرة: دار الثقافة للطباعة والنشر،1987) ص7.

2- أحمد خليفة الملط: **"الجرائم المعلوماتية"**، مرجع سابق ص 181.

3- حسن طاهر داود: "الحاسب وأمن المعلومات"، (الرياض:ب.د،2000) ص65.

د- إساءة استخدام البطاقات البنكية.

تعتبر الجرائم المتعلقة بإساءة استخدام البطاقات البنكية من الجرائم المتعلقة خصوصا فى المجتمعات التى تتسم نظمها البنكية بدرجة عالية من التطور والحداثة وتمنح فيها البطاقات النكية وكذلك تستخدم بأقل قدر ممكن من الإجراءات.

وتتحدد صور إساءة استخدام البطاقات البنكية فى:

1- استخدام البطاقات المسروقة أو منتهية الصلاحية.

2- تزوير البطاقات البنكية.

3- قيام صاحب البطاقة نفسه بسحب مبالغ نقدية أكبر من المبالغ المسموح له سحبها عن طريق ألة التوزيع الألى للنقود مستغلا بعض الثغرات التى مازالت تعانى منها الألات حتى الأن.

4- قيام بعض الأشخاص بإبلاغ البنك بضياع بطاقاتهم البنكية دون أن يكون ذلك صحيحا ثم يقومون على الفور بسحب النقود قبل أن يقوم البنك بالتحفظ على اموالهم وحمايتها، بحيث يعطوا انطباع بان سارق البطاقة أو من وجدها هو الذى قام بسحب النقود[1].

هـ- سرقة البيانات الشخصية.

وتتمثل سرقة البيانات الشخصية فى الاستيلاء على المعلومات المقدمة للجهاز (برامج أو بيانات للمعالجة) سواء كانت هذه البيانات مسجلة فى اسطوانات أو على

1- أحمد حسام طه تمام : "الجرائم الناشئة عن استخدام الحاسب، الحماية الجنائية للحاسب الألى "، **رسالة دكتوراه ،غير منشورة** (جامعة طنطا: كلية الحقوق،2000) ص210،211.

شريط ممغنط أو على ورق. كذلك يمكن الاستيلاء ماديا على الدعامة، الأمر الذى يبدو سهلا حيث أن سرقة هذه الدعامة لا تشغل إلى حيز زهيدا بالمقارنة بالاستيلاء على رزمة ملفات فى كراتين للإطلاع عليها يدويا، وحدث سنة 1967 فى احد المراكز المتخصصة فى المعالجة الألية للمعلومات أن سرق أحد الجناة بعض الاسطوانات وطلب فدية قدرها مائتان وخمسون ألف جنيها استرلينى من أجل اعادتها[1].

و- التلاعب فى برامج الأشخاص.

للبرامج أهمية عظمى فى مجال استخدام الحاسب الألى؛ لأن هذا البرنامج هو الذى يعطى الروح للحاسب فيجعله قادرا على القيام بما يناط به من أعمال.

على سبيل المثال.

الموظف المفصول الذى يتلاعب بالبرنامج حتى يتسبب فى افلاس المشروع الذى كان يعمل به انتقاما من المسؤلين عنه، وذلك بأن برمج جهاز الحاسب الألى بشكل يؤدى خلال 6 شهور إلى اخفاء كل البيانات المتعلقة بديون المشروع[2].

1- أحمد الطاهر النور: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية - الجرائم الإلكترونية غير الوطنية، بحث مقدم للندوة القانونية المتخصصة، الخرطوم 5،6 مارس 2000، ص12.

2- شمس الدين إبراهيم: **"وسائل مواجهة الإعتداء على الحياة الشخصية فى مجال تقنية المعلومات فى القانون السودانى"**،(القاهرة: دار النهضة العربية،2005) ص79.

وهناك بعض الجرائم المتعلقة بالبرامج منها:

1- تغيير برنامج نظام التشغيل.

حيث أن برنامج نظام التشغيل هو برنامج عام يحكم عمل الحاسب الألى نفسه والغش فى هذه الحالة يتحقق بتزويد البرنامج بمجموعة تعليمات اضافية، ويسهل الوصول إليها فقط بواسطة شفرة تتيح الحصول على جميع المعطيات التى يتضمنها الحاسب الألى.

2- خلق برنامج جديد.

حيث يقوم الجانى بذكاء بإعداد برنامج وهمى بأكمله.

3 - خلق برنامج وهمى.

نجد ان البرنامج قد صمم بأكمله من أجل ارتكاب الجريمة.

على سبيل المثال:

قيام إحدى الشركات الأمريكية بإصطناع وثائق تأمين لأشخاص وهميين بلغ عددها 6400 وثيقة، وزيادة فى التمويه زودت هذه الوثائق بتغييرات فى العناوين والأوضاع الاجتماعية مع اعتبار بعض المؤمن عليهم الوهميين أموات[1].

1- جميل عبد الباقى الصغير: " **القانون الجنائى والتكنولوجيا الحديثة: الكتاب الأول الجرائم الناشئة عن استخدام الحاسب الألى"**، ط1 (القاهرة: دار النهضة العربية، 1992) ص49، 48.

ز- جرائم القذف والتشهير.

مع تطور وسائل الاتصال واستخدام أجهزة الكمبيوتر المرتبط بعضها مع بعض بشبكة الإنترنت، والتقدم العلمى فى القدرة على بناء المواقع على هذه الشبكة واستعمال أسماء وهمية، والقدرة على انزال المعلومات المختلفة على هذه المواقع من دون معرفة مصدرها، وسرعة انتقال المعلومات والشائعات من خلال شبكة الإنترنت دون حسيب أو رقيب.

هذا التقدم الهائل فى شبكة الإنترنت واتساعها لتشمل جميع العالم جعلها موقعا خصبا لأصحاب الأهواء المريضة، والنفوس غير السوية وأصحاب الأغراض المشبوهة، فإتخذوا هذه الشبكة مكانا للتشهير بهم، والتعرض لحياتهم الخاصة دون موافقة صاحب العلاقة، بل وصل الأمر إلى التلصص على مواقع الأشخاص على شبكة الإنترنت والتسلل إليها وأخذ ما فيها من صور خاصة وأخبار، والعمل على نشر هذه الصور التى قد تمس الشرف[1].

ولم يقف الأمر عند هذا الحد، بل تعدى إلى الدول والشركات ونشر ما يلحق الضرر بها، ولايمكن أن يوصف هذا الفعل بأنه حرية رأى فالفرد الجهر بالحق وإسداء النصيحة للعامة والخاصة، بما يحقق المصلحة ويصون حقوق الفرد والمجتمع، ويحفظ النظام العام، ولكن هناك قيود لا ينبغى تجاوزها فى هذا الأمر منها.

- أن تمارس الحرية بأسلوب سلمى قائم على الدعوة إلى الله تعالى بالحكمة والموعظة الحسنة، ولا يجوز التعبير عن الرأى إذا كان فى ذلك اعتداء على حرمات الناس وراضهم.

فقد يعمل بعض الأشخاص من خلال شبكة الإنترنت على إبراز سلبيات بعض الأشخاص ونشر أسرارهم، أو نشر أخبار الشركات بما يلحق بها ضررا.

وقد يتم الحصول على هذه المعلومات بطرق غير مشروعة، أو بتلفيق الأخبار عنها، وحوادث التشهير والقذف على شبكة الإنترنت كثيرة ولا تحصى[2].

1- عارف خليل أبو عيد: "جرائم الإنترنت"، دراسة مقارنة، **مجلة جامعة الشارقة للعلوم الشرعية والقانونية**، المجلد 5، العدد 3 أكتوبر 2008.

2- محمد شلال العانى: " **التشريع الجنائى الإسلامى** "، ط2 (الأردن: مؤسسة المروة للطباعة،1993) ص165.

ح- جرائم المقامرة.

وتشمل تملك وادارة مشروع مقامرة على الإنترنت وتسهيل ادارة مشاريع القمار على الإنترنت وتشجيع مشاريع المقامرة على الإنترنت واستخدام الإنترنت لترويج الكحول ومواد الإدمان للقصر.

ط- الاحتيال الإلكترونى.

ويقصد به أى سلوك أو تصرف متعمد يحدث من فرد أو العديد من الأفراد يرهق او يتسبب فى أعباء اضافية على أية أطراف أخرى نتيجة استخدام ممارسات غير أخلاقية للحصول على ميزة غير عادلة أو غير قانونية.

وهناك العديد من الأسباب التى تؤدى إلى تفشى جريمة الإحتيال التجارى والتقليد وتتمثل هذه الأسباب فيما يلى:

1- غياب الوازع الدينى والأخلاقى لدى المصنعين والموردين للمنتجات.

2- ضعف نظام العقوبات الذى يطبق على المتعاملين بالسلع المقلدة.

3- عدم وجود شبكة ربط ألية بين الجهات المعنية بمكافحة هذه الظاهرة.

4- انعدام الخبرة لدى المتهاملين فى التجارة الإلكترونية وهى أهم وأكبر الأسباب التى تؤدى إلى تفشى هذه الظاهرة[1].

وهناك أشكال عديدة من الاحتيال منها.

1- الاحتيال فى التحصيل.

قد تتجه مؤسسات الأعمال إلى تنفيذ أنشطة المشتريات والتحصيل الإلكترونى وتنتاب عملية التحصيل الإلكترونى بعض مخاطر الاحتيال، نتيجة عدم وجود الرقابة الداخلية عندما يتم تنفيذ أنظمة التحصيل الإلكترونى.

2- الاحتيال على الحكومات.

يمكن أن تستفيد الحكومات من تكنولوجيا المعلومات والاتصالات فى تقدم وإدارة خدماتها إلكترونيا إلا أنها بمؤسساتها ووكالاتها الرسمية، أيضا قد تكون عرضة للاحتيال.

1- نهاد كريدى: **"الجريمة والاحتيال فى البيئة الإلكترونية"**، (بيروت: ب د،2008) ص 14،16.

3- احتيال المستهلك.

على الرغم من اتخاذ العديد من الاحتياطات لحماية المستهلك من التصرفات الاحتيالية على شبكة الانترنت إلا ان هناك تزايد فى أعداد الشكاوى التى تصدر من المستهلكين الذين يتعرضون لأفعال احتيالية على الانترنت[1].

1- حسنى عبد السميع ابراهيم: **"الجرائم المستحدثة على الانترنت"**، (القاهرة: دار النهضة العربية،2011) ص252،254.

ى- جريمة الاعتداء على حقوق الملكية الفكرية.

يعد الإنترنت من المجالات الهامة التى يظهر فيها بشكل واضح الاعتداء على حقوق اللكية الفكرية بشقيها الصناعى والأدبى، والتى تتضمن عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية الموضوعة على شبكة الإنترنت دون تفويض من صاحبها أو سداد قيمتها، واعادة استخدمها أو طبعا أو تسويقها باية صورة كانت[1].

مما يقتضى وجود قوانين خاصة تنظم مفردات الملكية الفكرية فى الفضاء الإلكترونى وتحميها من الإعتداءات التى تتعرض لها شأنها شأن الواقع المادى.

وقد ظهرت بعض المشكلات الخاصة بتطبيق حقوق الملكية الفكرية والعلامات التجارية وحق المؤلف على الإنترنت للأسباب الأتية:

1- تغير شكل وأسلوب إخراج وعرض المصنفات حيث أصبح الأمر يتعلق لمنظومة بيانات يتم نشرها على الإنترنت، ويمكن نسخها ونقلها وتحويلها بسهولة وسرعة فائقة، ويستطيع ملايين الأشخاص الحصول على نسخة كاملة من المصنف فى الحال[2].

2- أن الإنترنت شبكة مفتوحة مترامية الأطراف تتمتع بحرية وانسياب المعلومات دون أن تحكمها أى سلطة مركزية، ومن ثم لا توجد جهة محددة لتقصى التقليد أو النسخ الذى يشكل مساس بحقوق المؤلف.

1- محمد عبيد الكعبى: **"الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت"**، مرجع سابق ص 51.

2- عزة على محمد الحسن: **"الجريمة المعلوماتية فى القانون السودانى"** ص104،105.

3- أن قانون حماية الملكية الفكرية فى صورته التقليدية لا يصلح لمواجهة التحديات الجديدة؛ لأنه وضع لمواجهة صور النشر العادية وسبل الاعتداء المتعارف عليها على الصعيد الوطنى تحت رقابة السلطة المركزية المحلية، أما الأن فقد اختلف الأمر[1].

ك- جرائم غسيل الأموال.

مع نهاية القرن العشرينات برزت ظاهرة غسل الأموال عبر الإنترنت لتشكل معضلة كبيرة للنظم القانونية المعاصرة، ولعل السبب الرئيسى فى استجلاء هذه الظاهرة هى المدفوعات الافتراضية[2].

وغسل الأموال هو عبارة عن :

معالجة لمصدر الدخل الأول غير المشروع بالقيام بمجموعة تحركات اقتصادية مشروعة تؤدى إلى طبع الأموال غير المشروعة المصدر بطابع مشروع وبطريقة لايمكن بمقتضاها التعرف على المصدر الأصلى (غير المشروع).

وقد تطورت هذه الظاهرة مع ظهور شبكة الإنترنت واجتاحت العالم بأكمله، وذلك لكون الشبكة تمثل الوسيلة الفعالة والمسهلة لعمليات تبيض الأموال، وهذا ما جعل الأمر أكثر صعوبة بالنسبة للجهات المعنية فى متابعتها للمتعاملين عبر الشبكة وتحديد هويتهم، او جمع أيه بيانات أو معلومات عنهم.

1- محمد حسام محمود لطفى: "**المرجع العلمى فى الملكية الأدبية والفنية فى ضوء أراء الفكر وأحكام القضاء**"، ط1 (القاهرة :ب د،1992) ص197.

2- عمر بن يونس، يوسف أمين: "**غسل الأموال عبر الانترنت**"، ط1 (القاهرة :ب د،2004) ص31.

ويرجع السبب فى ذلك إلى[1].

1- أن شروط التعامل عبر الشبكة الدولية لا تتطلب اجراءات معقدة، إنما فقط تدوين الاسم ورقم بطاقة الإئتمان الخاصة بالمتعامل.

2- أن النقود الإلكترونية قد مكنت المتعاملين من تحويل مبالغ طائلة من دول أخرى بسهولة ودون مخاطر.

ل- جرائم المخدرات.

وهى جريمة أكثر خطورة حيث تهدد فئات المجتمع إذا أضحت الإنترنت قناة اتصالية ممتازة ومجالا رحبا للتعامل غير المشروع لمستهلكى المخدرات والمؤثرات العقلية، وهذا ما أدى إلى قيام عدة منظمات غير مشروعة تستخدم الإنترنت كوسيلة للترويج غير المشروع للمخدرات والمؤثرات العقلية سواء على المستوى المحلى او الإقليمى أو الدولى.

بل وأصبحت هناك مواقع لشرح التدريب على زراعة المخدرات وطرائق عمليات تحويلها خطوة بخطوة، وكذلك كيفية التعاطى لأول مرة والجرعات والمدة بين الجرعة والأخرى.

وتجدر الاشارة إلى أن أكثر الدول التى تنتشر فيها حركة الإتجار بالمخدرات والمؤثرات العقلية عبلا الإنترنت هى هولندا وسويسرا[2].

م- جرائم القدح والذم والتحقير عبر الإنترنت.

تعمل هذه المواقع على إبراز سلبيات الشخص المستهدف ونشر أسراره التى قد تم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، أو بتلفيق الأخبار عنه، وهناك حادثة مشهورة جرى تداولها بين مستخدمى الإنترنت فى بداية دخولها للمنطقة، حيث قام شخص فى دولة خليجية بإنشاء موقع ونشر صور إحدى الفتايات وهى عارية وفى أوضاع مخلة مع صديقها وقد حصل على تلك الصور من

1- نبيلة هبة هروال: **"الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات"**، مرجع سابق ص74.
2- عمر بن يونس: **"المخدرات والمؤثرات العقلية عبر الإنترنت"**،(الأسكندرية: دار الفكر الجامعى، 2004) ص46.

خلال التسل إلى حاسبها الشخصى، وحاول ابتزازها وهددها بنشر تلك الصور على الإنترنت وبالفعل قام بتنفيذ تهديده.

والقدح هو الإعتداء على كرامة الغير أو شرفه واعتباره ولو فى معرض الشك والاستفهام من دون بيان مادة معينة.

وحوادث القدح والتشهير على شبكة الإنترنت كثيرة، فقد وجد ضعاف النفوس فى شبكة الإنترنت فى ظل غياب الضوابط النظامية والجهات المسؤلة عن متابعة السلبيات التى تحدث فى أثناء استخدام الإنترنت متنفسا لأحقادهم ومرتعا لشهواتهم المريضة دون رادع أو خوف من المحاسبة[1].

1- على حبار االحسيناوى: **"جرائم الحاسوب والإنترنت"**،(عمان: دار اليازورنى، 2009) ص93.

ن- التجسس الإلكترونى.

فى عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائى، والعالم العربى والاسلامى كان ولا يزال أمنيا وثقافيا وفكريا لأسباب لا تخفى على أحد.

وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية خاصة مع استخدام الإنترنت وانتشاره عربيا وعالميا.

ولا تكمن الخطورة فى استخدام الإنترنت ولكن ضعف الوسائل الأمنية المستخدمة فى حماية الشبكات الخاصة بالمؤسسات والهيئات.

وتشارك فى تلك العمليات شبكة إشيلون المستخدمة فى التجسس على المكالمات ورسائل الفاكس والبريد الإلكترونى[1].

ويندرج تحته الإقتناء عن طريق وسائل غير مشروعة او الإفشاء أو النقل أو الاستعمال بدون وجه حق أو مبرر قانونى[2].

س- التهديد بالقتل.

فقد أدانت محكمة بفرنسا أحد الجناة بالحبس لمدة شهرين مع الإيقاف؛ لأنه بعث رسالة تهديد بالقتل عن طريق البريد الإلكترونى إلى أحد رجال السياسة.

كما تستخدم شبكة الإنترنت كوسيلة لإرتكاب درائم الضرب والجرح. فعلى أثر مشادة بين شخصين على أحد مجموعات المناقشة انتهت بمشاجرة فى ولاية نيوجرسى، حيث تمكن المتهم من تتبع عنوان المجنى عليه من خلال الإنترنت، ثم اصطحب زملائه إلى هذا العنوان واعتدوا على المجنى عليه بالضرب.

1- سامى على حامد عياد: **"الجريمة المعلوماتية واجرام الإنترنت"**،(الأسكندرية: دار الفكر الجامعى،2007) ص91.

2- هلالى عبد الله أحمد: **"التزام الشاهد بالإعلام فى الجرائم المعلوماتية"**، ط1(القاهرة: دار النهضة العربية،1997) ص21.

ع- القتل العمد.

وعلى سبيل المثال.

رجل قتل زوجته التى كانت موضوعة تحت المونيتور بأن دخل عن طريق الإنترنت إلى شبكة المعلومات الخاصة بالمستشفى، ثم قام بتغيير المعلومات الطبية الخاصة بالمجنى عليها (المريضة)[1].

ف- الدخول غير المشروع للحصول على بيانات تمس الأمن القومي أو الاقتصاد الوطني:

يكون قصد الجاني من التداخل أن يحصل على بيانات تمس الأمن القومي أو الاقتصاد الوطني وذلك من خلال الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني[2].

مثل ما حدث فى الولايات المتحدة الأمريكية من مهاجمة بعض القراصنة لمجلس الشيوخ والمباحث الفيدرالية والبيت الأبيض حتى أنهم يهاجمون البنتاجون 250 ألف مرة فى اليوم.

1- جميل عبد الباقى الصغير: " **الإنترنت والقانون الجنائى**"، (القاهرة: دار النهضة العربية،2001) ص41.
2- شيماء عبد الغني محمد عطا الله: " **مكافحة جرائم المعلوماتية في المملكة العربية السعودية**"، **بحث منشور على الانترنت** تاريخ الدخول2012/10/13 الساعة 2.30 عصراً

http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx

ص- الانترنت سلاح جديد للحرب.

فقد أصبح الانترنت سلاح يستخدمه الأعداء فى الحرب كما هو الحال فى الحرب العربية الإسرائيلية، حيث أقدم مجموعة من الشباب الاسرائيلين بمهاجمة موقع لحزب الله اللبنانى ونجحه فى تدميره لتتحول شبكة انترنت إلى ساحة قتال وقصف إلكترونى مكثف من مختلف مواقع العالم بين العرب والفلسطينين والمسلمين من جانب والإسرائيلين من جانب أخر، وطالت هذه الحرب إلى جانب مواقع السلطة الفلسطينية وحركة المقاومة الاسلامية وحركة حماس والمقاومة اللبنانية وحزب الله طالت مواقع الكنيست ووزارة الخارجية واضطرت وزارة الدفاع الإسرائيلية إلى الهجرة بمواقعها من خدمة (التلفزيون الإسرائيلية) لتعتمد على شركة (أى تى أند تى) الأمريكية[1].

ق- جرائم تتعلق بالتجارة الإلكترونية.

إن استخدام شبكة الإنترنت فى المعاملات التجارية والمصرفية والتعاقد عن بعد أدى إلى ظهور جرائم مستحدثة تتعلق بالإعتداء على التوقيع الإلكترونى الذى يتم عبر الإنترنت من خلال عملية التجارة الإلكترونية وهى تلك العملية التى تتم بين طرفين (بائع ومشترى) أو أكثر عبر الإنترنت

1- محمد فتحى: **"الإنترنت شبكة العجائب"**، (القاهرة: دار اللطائف، 2003) ص69-71.

ومن خلال معايير تحديد العمل التجارى يمكن تصور عدد الجرائم المرتكبة بالإعتداء على المعاملات التجارية وحركة التجارة وهذه المعايير لا تخرج عن أربعة معايير هى:

1- معيار المضاربة وقصد الربح.

2- معيار التداول.

3- معيار المقاولة.

4- معيار الحرفة التجارية[1].

1- محمد صلاح سالم: **"العصر الرقمى وثورة تكنولوجيا المعلومات"** ط1، (القاهرة: عين للدراسات والبحوث الانسانية والاجتماعية، 2002) ص182.

رابعاً: خصائص الجريمة الإلكترونية.

أ- الحاسب الألى أداه لإرتكابها.

ب- جريمة عابرة الحدود.

جـ- صعوبة اثباتها.

د- خصوصية الجريمة الإلكترونية.

هـ- خفاء الجريمة الإلكترونية.

و- سرعة التطور فى ارتكاب الجريمة الإلكترونية.

ز- أقل عنفا فى التنفيذ.

ح- جرائم ناعمة.

وفيما يلى شرح مفصل لخصائص الجريمة الإلكترونية:

أ- الحاسب الألى أداه لإرتكابها.

تعتبر هذه الخاصية من أهم الخصائص التى تميز الجرائم الإلكترونية عن غيرها من الجرائم الاخرى ولا سيما الجرائم التقليدية، ذلك لأن شبكة الإنترنت هى إحدى التقنيات الحديثة التى أفرزها تطور الحوسبة، ولذلك فإن ارتباطها بالحاسب الألى هو أمر لا مفر منه، باعتباره النفذة التى تطل بها تلك الشبكة على العالم الخارجى وإن كنا اليوم نعاصر امكانية استعمال الإنترنت عبر الهاتف الخلوى[1].

ب- جريمة عابرة الحدود.

يمكن القول ان من أهم ما يميز الجريمة الإلكترونية تخطيها للحدود الجغرافية ومن ثم اكتسابها طبيعة دولية، فبعد ظهور المعلومات، لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التى تتمتع بها الحاسبات الألية فى نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها ألاف الأميال، وقد ادت إلى نتيجة مؤداها أن اماكن متعددة فى دول مختلفة قد تتأثر بالجريمة الإلكترونية وحجم الأموال والمعلومات المستهدفة والمسافة التى قد تفصل الجانى عن هذه المعلومات والأموال، قد ميزت الجريمة الإلكترونية عن الجريمة التقليدية بصورة كبيرة[2].

جـ- صعوبة اثباتها.

1- أنها جريمة لا تترك أثر لها بعد ارتكابها.

2- صعوبة الإحتفاظ الفنى بأثارها إن وجدت.

1- نبيلة هبة هروال: **"الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الإستدلالات"**، (القاهرة: دار الفكر الجامعى،2007) ص35.

2- نائلة محمد فريد قورة: **"جرائم الحاسب الإقتصادية"**، دراسة نظرية وتطبيقية، (القاهرة: دار النهضة العربية، 2004) ص47.

3- أنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدى التعامل معها.

4- أنها تعتمد على الخداع والتضليل فى التعرف على مرتكبيها.

5- أنها تعتمد على الذكاء فى ارتكابها[1].

6- ترتكب من قبل شخص ذو دراية فائقة بالإنترنت.

7- سهولة اخفاء معالم الجريمة والتخلص من أثارها.

8- يلعب البعد الزمنى (اختلاف المواقيت بين الدول)، والبعد المكانى (تنفيذ الجريمة عن بعد)، والبعد القانونى (أى تطبيق القانون) دورا مهما فى تثبيت جهود التحرى والتنسيق الدولى لتعقب مثل هذه الجرائم[2].

د- خصوصية الجريمة الإلكترونية.

تتميز هذه الجريمة بقلة عدد الحالات التى يتم اكتشافها بالفعل إذا ما قارنا ذلك فى ضوء ما تم اكتشافه من الجرائم التقليدية، ويرى البعض أن من بين الأسباب وراء صعوبة اكتشاف هذه الجرائم يرجع إلى تميزها بأنها لايشوب ارتكابها أى عمل من أعمال العنف كما أنها لا تترك أثارا.

وكذلك وسيلة تنفيذها التى تتسم فى أغلب الحالات بالطابع التقنى الذى يضفى عليها الكثير من التعقيد. بالإضافة إلى الإحجام عن الإبلاغ عنها فى حالة اكتشافها لخشية المجنى عليهم من فقد ثقة عملائهم، فضلا عن إمكانية تدمير المعلومات التى يمكن أن تستخدم كدليل فى الإثبات مدة لاتقل عن الثانية الواحدة[3].

1- www .Minshawi .com 2011/1/3 (مصدر) تاريخ الدخول

2- منير محمد الجهينى، ممدوح محمد الجهينى: **جرائم الإنترنت والحاسب الألى ووسائل مكافحتها"**، القاهرة: دار الفكر الجامعى،2004) ص16.

3- هشام محمد فريد رستم: **"قانون العقوبات ومخاطر تقنية المعلومات"**، (أسيوط: مكتبة الألات الحديثة،1994) ص42،41.

هـ- خفاء الجريمة الإلكترونية.

تتسم الجرائم الإلكترونية بانها مستترة خفية فى أغلبها، حيث أن المجنى عليه لا يلحظها غالبا مع أنها تقع أثناء وجوده على الشبكة ولكن لايكون عالما بها ولا ينتبه إلبها إلا بعد فترة من وقوعها وفى بعض الأحيان لايكتشف أمرها.

كما أن توافر المعرفة والخبرة التقنية لدى الجانى فى هذا المجال يؤدى إلى صعوبة اكتشاف جريمته، وذلك باتباعه لطرق وأساليب لايفطن إليها المستخدم العادى للشبكة مثل ارسال فيروسات مدمرة، سرقة أموال وبيانات، تجسس وغيرها[1].

و- سرعة التطور فى ارتكاب الجريمة الإلكترونية.

التطور السريع الذى تشهده تكنولوجيا المعلومات أضفى بظلاله على الجرائم الناشئة عن الإنترنت حيث أن أساليب ارتكابها دائما فى تطور مستمر، وأن المجرمين فى مختلف أنحاء العالم يستفيدون من الشبكة فى تبادل الأفكار والخبرات الإجرامية فيما بينهم.

ز- أقل عنفا فى التنفيذ.

جرائم الإنترنت لاتحتاج إلى عنف عند تنفيذها، أو مجهودا كبيرا، وانما تنفذ بأقل مجهود ممكن، حيث يعتمد الجانى وبشكل رئيسى على الخبرة فى المجال المعلوماتى، وهذا عكس الجرائم التقليدية التى تحتاج إلى عنف ودماء ومجهود كبير يقوم به الجانى غالبا فى الوصول إلى غايته[2].

1- محمد عبيد الكعبى: **"الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت"**، ط2 (القاهرة: دار النهضة العربية، 2009) ص38.

2- محمد عبد الرحيم سلطان: "جرائم الإنترنت والإحتساب عليها"، **مؤتمر القنون والكمبيوتر والإنترنت** (العين: جامعة الإمارات، مايو 2002).

ح- جرائم ناعمة.

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل السرقة، الاغتصاب، فالجرائم الالكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد عل الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية بالحاسب الآلي[1].

1- مصدر الدخول 2012/11/10 الساعه 1 ظهراً http:http://form.biskra7.com

خامساً: أضرار الجريمة الإلكترونية.

نظرا لوقوع الجرائم الإلكترونية فى نطاق تقنية متقدمة وأنها تتزايد يوما بعد يوم، وأن مجالات وقوعها كثيرة ومخاطرها عديدة نظرا لطبيعة استخدامها فى المعاملات الإقتصادية والمالية والوطنية والدولية والإعتماد عليها فى تيسير شئون الحياة اليومية بالنسبة للأفراد والشئون العامة بالنسبة للحكومات، ومن شأن ذلك أن يضفى أبعادا غير مسبوقة على الخسائر والأضرار التى تنجم عن هذه الجرائم ويدل على ذلك أن الخسائر المادية الناجمة عن هذه الجرائم ضخمة جدا[1].

كذلك هذه الأضرار قد تصيب النظام المعلوماتى بصفة عامة، وتؤدى إلى تدمير النظام بصفة كلية أو جزئية قد تكون طبيعية أو من فعل الإنسان، حيث يكون النظام المعلوماتى مستهدف بغرض تدميره أو تعطيله أو جعله غير صالح للإستعمال مؤقتا.

وتتمثل مخاطر المعلوماتيه فى نوعين من المخاطر.

أ- مخاطر عمدية.

ب- مخاطر غير عمدية[2].

وتتمثل المخاطر العارضة او الغير عمدية فى الأضرار الناشئة عن العوامل الطبيعية مثل خلل كهربائى وتؤدى إلى الإتلاف الجزئى أو الكلى للمعدات المعلوماتية والدعائم التى تختزن المعلومات، أو تعطل المعدات والكايانات المنطقية حتى لو كانت لفترة زمنية قصيرة، وكذلك الأخطاء الخاصة بنقل واستعمال المعلومات وهو أمر وارد طالما أن الإنسان يتدخل فى عملية معالجة المعلومات وأخطاء التشغيل وأخطاء التصميم والتنفيذ[3].

1- أحمد خليفة الملط : **"الجرائم المعلوماتية: دراسة مقارنة"**، ط1(القاهرة:دار الفكر الجامعى،2006) ص95.
2- خالد محمد كدفور المهيرى: **"جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية"**، (دبى: دار العزيز للطباعة والنشر،2005) ص118.
3- خالد ممدوح إبراهيم: **"أمن الجريمة الإلكترونية"**، (الدار الجامعية، 2010) ص55.

سادساً: أسباب زيادة الجرائم الإلكترونية فى مصر والوطن العربى.

أ- ضعف الوازع الدينى والفهم الخاطىء لبعض أمور الدين.

يقدم بعض الإفراد لارتكاب مثل هذه الجرائم بسبب ضعف الوازع الدينى، كذلك تستغل بعض المواقع الدافع الجهادى بإسم الدين ويتزامن ذلك مع وجود بعض المشكلات السياسية والإقتصادية على الصعيدين العربى والإسلامى والتى ادت إلى زيادة الترويج لهذه المواقع مما أدى إلى ظهور ما يعرف بالجهاد الإلكترونى (Jihadonline).

ودائما يبحث أصحاب هذه المواقع عن المواهب الشابة التى تساعدهم فى إدارة المواقع واستخدام التقنيات الحديثة، ويتم استقطابهم بداية بإسم الوازع الدينى والذى ربما يتحول فيما بعد بأساليب مختلفة إلى دافع إرهابى[1].

ب- زيادة قاعدة مستخدمى الإنترنت فى الوطن العربى.

مع انتشار خدمات الإنترنت وانخفاض تكلفة الإشتراكات، بدأت قاعدة المستخدمين فى الزيادة بشكل ملحوظ مقارنة بدول العالم الأخرى وهذا العدد الكبير جدا من المستخدمين للإنترنت فى المنطقة، جعل الإنترنت الأكثر شعبية، ووسيلة مريحة للإتصال، كما أنها فتحت أبوابا جديدة للأعمال على الإنترنت، ففى مصر بلغ عدد مستخدمى الإنترنت 11.48مليون مستخدم، إلا ان إساءة الاستخدام زاد أيضا بسبب عدم وجود برامج توعية، لذا فقد أصبح الكثيرون من مستخدمى الإنترنت فى المنطقة ضحايا للاختراقات والجريمة الإلكترونية.

1- www Wikipedia..com 2009/9/1 (مصدر) تاريخ الدخول

جـ- مشكلة البطالة.

مشكلة البطالة من المشكلات التى يعانى منها الشباب وأغلبهم من خريجى الجامعات الذين يتمتعون ولو بقدر ضئيل من أساسيات استخدام الكمبيوتر والإنترنت، وإذا لم يكن لديهم انترنت فى المنزل فهم يلجئون إلى مقاهى الإنترنت، والتى تنتشر بشكل كبير فى كل دول المنطقة وكل هذه العوامل تتكاتف بشكل ملحوظ؛ لزيادة حجم الجريمة الإلكترونية، وظهور ما يسمى بمجرمى الإنترنت المحليين؛ أى من داخل المنطقة نفسها وليس من خارجها، وهؤلاء يمثلون الخطر الأكبر فلديهم الوقت الكبير، ومنهم من لديه الدافع الدينى، ومنهم من يعمل للدافع المادى، خاصة مع انتشار المواقع العربية التى تقدم خدمات تعليم الإختراق.

د- ضعف القوانين الرادعة.

بعض البلاد العربية لديها قوانين متخصصة فى الجريمة الإلكترونية، والقليل من البلدان تحاول سن تشريعات لهذا النوع من الجرائم، إلا أنها مازالت فى مراحلها الأولى، وتحتاج إلى المزيد من التحسينات والتنقيح، وبسبب المشكلات السياسية فى المنطقة فإن معظم الدول تلجأ إلى استخدام مايعرف بقوانين الطوارىء (Emergency Laws) عوضا عن قوانين متخصصة للجريمة الإلكترونية كأسلوب من أساليب الردع لهذا النوع من الجرائم.

على سبيل المثال:

القبض على المدونين بتهم السب والقذف وغيرها.

هــ- القصور فى برامج التوعية الأمنية.

برامج التوعية بأمن المعلوملات من أكثر الطرق فعالية فى محاربة الجرائم الإلكترونية، فهناك نقص شديد جدا فى برامج التوعية بأمن المعلومات على مستوى الأفراد والمؤسسات والحكومات. وقد يستغل المجرمون عوامل قلة برامج التوعية بأمن المعلومات فى ارتكاب مثل هذه الجرائم، خصوصا وأنن هذه البرامج متوفرة باللغة الإنجليزية، لذا فإن هناك حاجة إلى برامج توعية وتدريب تستهدف الناطقين باللغة العربية لتدريب المستخدمين والعاملين فى الشركات، ورجال القانون، لفهم المشكلة وتداركها سريعا[1].

وما يجدر الإشارة إلية أنه بما أن هناك جريمة فلابد من مرتكب لهذه الجريمة أو ما يسمى بالمجرم الإلكترونى.

1- www.Knwledge Society,in Wikipedia.org (مصدر) تاريخ الدخول 2012/3/16

سابعاً: ماهية المجرم الإلكترونى.

المجرم الإلكترونى مجرم أو عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يبين أن المجرم الذي يرتكب الجريمة المعلوماتية هو مجرم في الغالب متخصص في هذا النوع من الإجرام[1].

1-http:// sy-street.net مصدر تاريخ الدخول 2012/9/28 الساعه 12.30 صباحاً

ثامناً: خصائص المجرم الإلكترونى.

أ- مجرم المعلومات مجرم متخصص.

فقد ثبت فى العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أى انهم متخصصون فى هذا النوع من الجرائم.

ب- المجرم المعلوماتى مجرم عائد إلى الإجرام.

حيث يعود كثير من مجرمى المعلومات إلى ارتكاب جرائم أخرى فى مجال الكمبيوتر انطلاقا من الرغبة فى سد الثغرات التى أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة فى المرة السابقة، ويؤدى ذلك إلى العودة إلى الإجرام، وقد ينتهى بهم الامر فى المرة التالية إلى تقديمهم إلى المحاكمة[1].

جـ- المجرم المعلوماتى مجرم محترف.

ذلك أنه لايسهل على الشخص العادى إلا فى حالات قليلة، أن يرتكب جرائم بطريق الكمبيوتر فالأمر يقتضى كثير من الدقة والتخصص فى هذا المجال للتوصل إلى التغلب على العقبات التى أوجدها المتخصصون لحماية أنظمة الكمبيوتر، كما يحدث فى البنوك على سبيل المثال[2].

1- عبد الفتاح بيومى حجازى: **"مبادىء الإجراءات القانونية فى جرائم الكمبيوتر والإنترنت"**، ط1 (القاهرة: دار الفكر العربى، 2006) ص45- 46.

2- غنام محمد غنام: **"عدم ملاءمة القواعد التقليدية فى قانون العقوبات لمكافحة جرائم الكمبيوتر"، مؤتمر القنون والكمبيوتر والإنترنت**. جامعة الإمارات:كلية الشريعة والقانون،2000) ص1.

د- الذكاء.

يعتبر الذكاء من أهم صفات مرتكب الجرائم الإلكترونية لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الألى والقدرة على التعديل والتغيير فى البرامج وإرتكاب جرائم السرقة والنصب وغيرها من الجرائم التى تتطلب أن يكون مرتكب الجريمة على درجة كبيرة من المعرفة لكى يتمكن من إرتكاب تلك الجرائم، وتتجلى اهمية صفة الذكاء بالنسبة لمرتكب الجريمة الإلكترونية فى عدم استخدامه للعنف فى إرتكاب الجريمة لأنه يستطيع وهو فى منزله تحويل عدة ملايين من الجنيهات لحسابه من بنك إلى أخر أو فى نفس البنك[1].

هـ- الخبرة والمهارة.

يتصف مرتكب الجرائم الإلكترونية بانه على درجة عالية من الخبرة والمهارة فى استخدامه التقنية المعلوماتية وذلك لأن مستوى الخبرة والمهارة التى يكون عليها هى التى تحدد الأسلوب الذى يرتكب به تلك الجرائم، بحيث إذا كان الشخص مرتكب الجريمة على قدر ضئيل من مستوى الخبرة نجد أن الجرائم التى قد يرتكبها لا تتعدى الإتلاف المعلوماتى إما بالمحو أو بالإتلاف وكذلك بنسخ البيانات والبرامج.

أما إذا كان الشخص على درجة أعلى فى المستوى المهارى فإن أسلوب إرتكابه للجرائم يختلف، حيث يقوم عن طريق استخدام الشبكات بالدخول على أنظمة الحاسب الألى وسرقة الأموال وإرتكاب جرائم النصب وإرتكاب جرائم التجسس وزرع الفيروسات وغيرها من الجرائم التى تتطلب مستوى مهاري وخبرة كبيرة فى إرتكابها[2].

1- أيمن عبد الحفيظ: "**الإتجاهات الأمنية والفنية لمواجهة الجرائم المعلوماتية**"، (القاهرة: ب.د، 2005) ص14،13.
2- أحمد ضياء: " **الظاهرة الإجرامية بين الفهم والتحليل**"، (القاهرة: دار النهضة العربية،2001) ص 294- 295.

و- المجرم الإلكترونى إنسان إجتماعى.

لا يضع المجرم المعلوماتى نفسه فى حالة عداء سافر مع المجتمع الذى يحيط به، بل أنه إنسان متوافق معه، ذلك لأنه فى الأساس انسان مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء فى نظر الأخرين ليس سوى القدرة على التكيف ولا يعنى ذلك التقليل من شأن المجرم الإلكترونى بل طورته الإجرامية قد تزداد إذا زاد تكيفه الإجتماعى مع توافر الشخصية الإجرامية لديه[1].

ز- الميل إلى التقليد.

يبلغ الميل إلى التقليد منهاه حين يوجد الفرد وسط اخرين مجتمعين، إذ يكون عندئذ أسهل وأسرع انسياقا لتأثير سواه عليه[2].

ويظهر ذلك فى مجال الجريمة المعلوماتية لأن أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية التى لديه مما يؤدى به الأمر إلى إرتكاب الجرائم[3].

1- أيمن عبد الحفيظ عبد الحليم سليمان: **"استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الألى"، رسالة دكتوراه غير منشورة** (أكاديمية الشرطة، 2004) ص49.

2- رمسيس بهنام: **" المجرم تكوينا وعقيدة"**، (الأسكندرية: منشأة دار المعارف،ب ت) ص176، 177.

3- أيمن عبد الحفيظ : **"الإتجاهات الأمنية والفنية لمواجهة الجرائم"**، مرجع سابق ص15.

تاسعاً: فئات المجرم الإلكتروني.

أ- الهواه.

ب- الهاكرز.

جـ- المجرمون المحترفون.

د- الكركر.

هـ- طائفة صغار السن (صغار النوابغ).

و- المجرمون البالغون.

ز- الحاقدون[1].

1-http://coeia.edu.sa/index.php/ar/asuurance-awamess/articles/51-forensic-and-computer-crimes/ (مصدر) تاريخ الدخول 2012/22

وفيما يلى شرح مفصل لفئات المجرم الإلكترونى:

أ- الهواه.

وهم الشباب الذين انبهروا بالثورة المعلوماتية وانتشار الحاسبات الألية وهؤلاء الشباب لديهم قدرا لابأس به من الخبرة المعلوماتية لذلك فهم يمارسون مواهبهم فى استخدام الحاسب الألى بغرض اللهو او هواية اللعب من اجل الوصول إلى نظم المعلوماتية سواء الخاصة بالوزارات أو الشركات العملاقة أو الشركات التجارية أو المؤسسات المصرفية أو المؤسسات العسكرية كنوع من التحدى وإثبات المهارات الذاتية والتفوق والذكاء الشديدين، فهؤلاء الشباب تكون غايتهم فى النهاية مجرد التسلية وليس لديهم النيه لإرتكاب أفعال جريمة ما عبر الشبكة الدولية للمعلومات ومع ذلك فقد يتطور الأمر أحيانا إلى إنزلاق هؤلاء الشباب من مجرد هواه إلى محترفين للأفعال الغير مشروعة وارتكاب تلك الجرائم[1].

1 -David I Cave&William Vastorch:**Computer Crime Acrime Fight** (Reilly&Associate, nc1995)p 61.

ب- الهاكرز.

هم الاشخاص الذين يخترقون الجهاز فيستطيعون مشاهدة ما به من ملفات او سرقتها. ولا يستطيع الهاكر الدخول الى جهازك الا مع وجود ملف يسمى (Patch) او (TROJAM) وهذه الملفات هي التي يستطيع الهاكر بواسطتها الدخول الى جهازك الشخصي حيث يستخدم الهاكر احد برامج التجسس التي ترتبط مع ملف (Batch) الذي يعمل كـ (ريسيفر) يستطيع ان يضع له الهاكر (اسم مستخدم) و(رمز سري) تخوله ان يكون هو الشخص الوحيد الذي يستطيع الدخول الى جهازك وكذلك يستطيع ان يجعل جهازك مفتوحاً فيستطيع اي هاكر ان يدخل الى جهازك[1].

فهم دائما يستهدفوا الدخول إلى انظمة الحاسبات الألية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض وذلك بهدف اكتساب الخبرة وبدافع الفضول، أو لمجرد اثبات القدرة على إختراق هذه الأنظمة[2].

جـ- المجرمون المحترفون.

تتميز هذه الفئة بسعة الخبرة، والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التى ترتكب من قبل أفرادها، لذلك فإن هذه الطائفة تعد الأخطر من بين مرتكبى الجرائم الإلكترونية، حيث تهدف إعتداءاتهم إلى تحقيق المكسب المادى لهم او للجهات التى كلفتهم وسخرتهم لإرتكاب مثل هذه الجرائم، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكرى أو نظرى أو فلسفى.

1- هنا أبو جريشة الحداد: "الجريمة الإلكترونية فيرس - قرصنه – احتيال" **بحث منشور على الانترنت** تاريخ الدخول 2012/10/13 الساعة 3 عصرا www.lipa-lb.org

2- أحمد سمير: الجريمة المعلوماتية **بحث منشور على الإنترنت** فى نوفمبر 2010 مصدر تاريخ الدخول 2010/10/13 الساعة 3 عصرا www. http://www.babylon.com

د- المجرمون البالغون.

بعض الدراسات تشير إلى أن أكثر الفئات العمرية التى ترتكب مثل هذه الجرائم تنتمى إلى فئة عمرية تتراوح بين (25-45) عاما، وبالتالى تكون أغلب هذه الفئة من الشباب، إذا استثنينا صغار السن من بينهم الذى تكون أعمارهم دون الحد الأدنى المشار إليه[1].

هـ- الكركر.

أو الهاكرز الخبيث أو المحترف ذو النوايا الإجرامية، ولقد برز هذا المصطلح مع العام 1985 ودوره القيام بكل ماهو سىء وشرير وما يشكل جريمة سواء كان إتلافا أو تخريبا أو ارهابا او ابتزاز أو عدوان على الأموال بالنصب او السرقة أو التهديد المباشر والكامل للمصالح عبر الإنترنت ولا يتوانى عن إرتكاب جريمة فى كل الظروف لان الذى يحكمه فكرة البطولة الطفولية. ولعل المظهر الخطر فى نوعية الهاكرز الخبيث أن قسما من هذه النوعية لا يدرك خطورة عمله وهو ما يطلق عليه أحيانا بسمة الأطفال المهرة للدلالة على براءتهم حيث يرتكب أعمالا خطرة عبر الإنترنت فى الوقت الذى لايدرك فيه مدى خطورتها[2].

1- مديحة فخرى محمود محمد: **" دور الجامعات المصرية فى مواجهة الجرائم الإلكترونية"، رسالة دكتوراه غير منشورة** (جامعة حلوان:كلية التربية،2011) ص10

2- عمر محمد أبوبكر بن يونس: **" الجرائم الناشئة عن استخدام الإنترنت الجوانب الموضوعية والإجرائية"**، (القاهرة: دار النهضة العربية،2004) ص141،140.

و- طائفة صغار السن (صغار النوابغ).

يقصد بهم الشباب البالغ الذى فتن بالمعلوماتية والحاسبات الألية، وقد لفتوا النظر فى الأونة الأخيرة فى بعض أفعال الإنتهاك لنظم المعلوماتية، ولا سيما وأنه لاتوجد حدود جغرافية لأفعالهم التى تصل إلى أنظمة ومراكز المعلوماتية التى توجد على بعد ألاف الأميال من أماكن تواجدهم[1].

ز- الحاقدون.

هذه الطائفة يغلب عليها عدم توفر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين، فهم لا يسعون إلى اثبات القدرات التقنية والمهارية وفى نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية، إنما يحرك أنشطتهم الرغبة فى الإنتقام والثأر كالثأر من تصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لايكونوا موظفين فيها.

ولهذا فإنهم ينقسمون إما إلى مستخدمين للنظام بوصفهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، او إلى غرباء عن النظام يتوفر لديهم الإنتقام من المنشأة المستهدفة فى نشاطهم.

ولا يتسم أعضاء هذة الطائفة بالمعرفة التقنية والإحترافية وتغلب أنشطتهم على البرامج الضارة وتخريب النظام أو إتلاف نعطياته وتقنيات زراعة الفيروسات وهم أقل خطورة من غيرهم من مجرمى التقنية[2].

1- محمد سامى الشوا: **" ثورة المعلومات وانعكاستها على قانون العقوبات"**، (القاهرة: دار النهضة العربية،1994) ص7.

2- أيمن عبد الله فكرى: **"جرائم نظم المعلومات"**، رسالة دكتوراه غير منشورة، (جامعة المنصورة: كلية الحقوق،2006) ص81.

عاشراً: دوافع مرتكب الجريمة الإلكترونية.

أ- استكشاف عالم شبكة المعلومات الدولية.

ب- السعى إلى الربح.

جـ- الإرهاب والتجسس.

د- إثبات التفوق العلمى.

هـ- الإنتقام.

و- إرتكاب الجرائم كوسيلة للدعاية.

ز- الغرور و المتعة.

ح- الشعور بالنقص.

وفيما يلى شرح مفصل لهذه الدوافع:

أ- استكشاف عالم شبكة المعلومات الدولية.

نظرا للثورة التكنولوجية الحديثة وانتشارها فى المجتمعات المتقدمة بصورة هائلة وما أدى ذلك إلى انبهار بعض المجرمين بهذه التقنية الحديثة إن كانوا ليسوا على درجة كبيرة من الخطورة الإجرامية إذ أنه لايتوافر لديهم أى نوايا سيئة إلا أن غايتهم عند ارتكاب مثل هذه الجرائم هى غاية التعلم.

ويرى بعض الباحثين ان الدافع قد يكون الرغبة فى قهر أنظمة الشبكة، حيث يميل مرتكبى هذه الجرائم فى حالة ظهور تقنية حديثة إلى اظهار تفوقهم وبراعتهم، فيحاولون ايجاد الوسيلة إلى تحطيم تلك التقنية أو التفوق عليها ويتزايد شيوع هذا الدافع لدى فئة صغار السن[1].

1-http://www.arablaw.org/ 2011/4/12 تاريخ الدخول (مصدر).

ب- السعى إلى الربح.

إن مجرم الشبكة الدولية للمعلومات عندما تتجه غايته إلى تحقيق الربح فليس هناك أسهل من الإلتجاء إلى الشبكة الدولية للمعلومات وذلك على سبيل المثال بإختراق أحد أنظمة البنوك والإستيلاء على مبالغ مودعة لدى البنك لحساب عميل لديها، وقد يلجأ إلى الإبتزاز عن طريق الإستيلاء على برامج معينة أو معلومات سرية حصل عليها بأى صورة[1].

جـ- الإرهاب والتجسس.

هناك دافع أخر لإرتكاب جرائم شبكة للمعلومات الدولية وهو الإرهاب والتجسس، فمحرك أنشطة الإرهاب الإلكترونى وحروب المعلومات هى الدوافع السياسية والأيديولوجية.

أما التجسس فمع عصر التقنيات العالمية أصبحت حدود الدول مستباحة لتوفر الأقمار التجسسية والبث الفضائى، فضلا عن عمليات التجسس التى تقوم بها الأجهزة الإستخباراتية للحصول على أسرار ومعلومات الدولة ومن ثم إفشائها لدول أخرى معادية واستغلالها بما يضر بالمصلحة الوطنية، وهناك شكل أخر من التجسس فى المجال التجارى والصناعى ويكون الهدف منها الإستيلاء على الأسرار التجارية والصناعية والعلامات التجارية وبراءات الإختراع وكلها تحركها دوافع المنافسة[2].

د- إثبات التفوق العلمى.

يقوم المجرم بمحاولة اثبات التفوق العلمى من خلال التحدى الفكرى أثناء استخدامه للحاسب الألى واثباته قدرته على اختراق أنظمة والدخول عليها وهو أحد الدوافع التى تجعل الكثير يلجأون إلى ارتكاب مثل تلك الأفعال على الرغم من عدم توافر نيه ارتكاب الجريمة.

1- محمد على العريان: **"الجرائم المعلوماتية"**، ط1 (الأسكندرية: دار الجامعة الجديدة، 2004) ص66.

2 - منى فتحى أحمد عبد الكريم: **"الجريمة عبر الشبكة الدوليه صورها ومشاكل اثباتها"**، رسالة دكتوراه غير منشورة (جامعة القاهرة: كلية الحقوق، 2007) ص 29،28.

ولذلك فإن أغلب من يقومون بتلك الأفعال بدافع اثبات التفوق العلمى هم الصبية والشباب أو ما يعرف بإسم صغار نوابغ المعلوماتية لأن هؤلاء يسعون دائما إلى اكتشاف ما هو جديد ومحاولة التعامل مع هذه البرامج الجديدة واثبات تفوقهم العلمى عن طريق تخطى حاجز الحماية لهذه البرامج غير عابئين بما يحدث من مشاكل أو كوارث[1].

وقد أظهرت الدراسات الحديثة أن هذا الدافع يسود على غيره من الدوافع ويعكس اتجاه مجرمى التقنية إلى السعى لتحقيق مكاسب مادية شخصية[2].

هـ- الإنتقام.

يعد دافع الإنتقام من أخطر الدوافع التى يمكن أن تدفع الشخص إلى ارتكاب جريمة لأن الإنتقام غالبا يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التى يعمل بها لأنه غالبا ما يكون أحد موظفيها ويقوم بهذا الدافع وهو غرض الإنتقام نتيجة لفصله من العمل أو تخطيه فى الحوافز او الترقية، ومما يزيد من خطورة الأمر هو قيام أحد هؤلاء الموظفين بالإستعداد مسبقا لمثل هذا الموقف، حيث يقوم بزرع برنامج يحمل تعليمات لمسح كافة البيانات فى حالة عدم وجود اسمه فى كشف الموظفين بالشركة، ويقوم عند فصله بالإنتقام من هذه المؤسسة عن طريق تشغيل هذا البرنامج[3].

و- إرتكاب الجرائم كوسيلة للدعابة.

يعتبر دافع المزاح أو الدعابة التى تجعل الشخص يقوم بتصرفات وان كان لايقصد من وراءها إحداث جرائم وإنما بغرض المزاح فقط، ولكن هذه التصرفات قد ينتج عنها نتائج ترقى إلى درجة الجريمة.

1- انتصار أنور الغريب: "**أمن الكمبيوتر والقانون**"،(بيروت:دار الراتب الجامعية،1994) ص10.

2 - http://www.arablaw.org/ 2011/2/1 تاريخ الدخول (مصدر).

3- محمد سامى الشوا: "**ثورة تكنولوجيا المعلومات**"، مرجع سابق ص531.

فعلى سبيل المثال:

قيام شخص بمسح معلومات مهمة فلا يمكن القول بأن هذا التصرف مجرد دعابة، بل إن هذا التصرف فى حقيقته هو جريمة إتلاف وتخريب متعمد[1].

ز- الغرور والمتعة.

يتولد لدى طائفة من المجرمين صفة الغرور والمتعة، حيث يقدم المجرم على ارتكاب الجريمة تعاليا وتفاخرا بقدرته على احداث الأثار المترتبة عليها.

ويرتبط هذا بالمتعة بصرف النظر عن حجم الخسائر والأضرار المترتبة على جريمته ويمكن التمييز بين الشخص المغرور الذى قد لايكون على درجة علمية كبيرة والشخص المتفوق علميا الذى يسعى لإبراز كفاءته امام الغير بما لديه من معلومات[2].

ح- الشعور بالنقص.

يعد الشعور بالنقص من العوامل المؤثرة فى إقدام المجرم على ارتكاب جريمته وقد يكون هذا الشعور بالنقص سواء تعلق ذلك بالناحية الفسيولوجية أو النفسية أو العلمية مما يؤدى إلى شعور الفرد بأنه أقل مستوى من الأخرين مما يؤدى إلى محاولة اثبات ذاته وتغلبه على هذا النقص بإظهار تفوقه فى مجال أخر تعويضا عن العجز الذى يعانيه[3].

فمثلا لوحظ أن العاملين فى قطاع التقنية او المستخدمين فى قطاعات العمل الأخرى يتعرضون على نحو كبير لضغوط نفسية ناجمة عن ضغط العمل والمشكلات المادية، وتتجه للعمل على الحاسب الألى منفردا لفترات طويلة هذه الأمور قد تدفع إلى ارتكاب جرائم الشبكة الدولية للمعلومات وباعثها هو البحث عن الإثارة والمتعة والتحدى[4].

1- أيمن عبد الحفيظ : **"الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية"**، مرجع سابق ص20.
2- رمسيس بهنام: **"المجرم تكوينا وعقيدة"** ،(الأسكندرية: منشأة دار المعارف، ب ت) ص175.
3- رمسيس بهنام: **" المجرم تكوينا وعقيدة"**، مرجع سابق ص175.
4- محمد عبد الله المنشاوى: **جرائم الإنترنت من منظور شرعى وقانونى، بحث منشور على الإنترنت** (مصدر) تاريخ الدخول 2011/1/15 www .Minshawi .com

ولكى تتم الجريمة الإلكترونية لابد من توافر ثلاثة عناصر لدى الجانى حتى يتدخل تدخلا غير مشروع فى ذاكرة الحاسب:

1- أن يحوز بنفسه حاسبا أليا، ونهاية طرفية عبارة عن محطة للتراسل بين المستعمل - المستخدم والحاسب الألى، أو ان يكون لدية شفرة على الأقل.

2- أن يكون لدية موديم (Modem) وهو عبارة عن أدلة لترجمة تعليمات مكتوبة بلغة الحاسب الألى إلى رموز رقمية أو العكس، حيث يسمح للحاسبات الألية أن تستقبل وتنقل المعلومات عن طريق وسيط لخط تليفون.

3- أن يكون لديه قدرا لابأس به من الحيل والكفاءة[1].

ويمكن تصنيف الجرائم الإلكترونية حسب دور الحاسب الألى فيها، حيث يلعب الحاسب الألى ثلاثة أدوار فى ميدان إرتكاب الجرائم الإلكترونية، ودورا رئيسيا فى حقل اكتشافها:

أ- قد يكون الكمبيوتر هدف للجريمة.

ب- قد يكون الكمبيوتر اداة لإرتكاب الجريمة.

جـ- قد يكون الكمبيوتر بيئة لإرنكاب الجريمة.

1- عبد الفتاح بيومى حجازى: **مكافحة جرائم الكمبيوتروالإنترنت فى القانوت العربى النموذجى"**، ط1 (القاهرة: دار الفكر العربى، 2006) ص89.

وفيما يلى شرح مفصل لدور الكمبيوتر فى الجريمة الإلكترونية واكتشافها:

أ- قد يكون الكمبيوتر هدفا للجرائم Target Of An Offens

وذلك كما في حالة الدخول غير المصرح به الى النظام او زراعة الفايروسات لتدمير المعطيات والملفات المخزنة او تعديلها، وكما في حالة الاستيلاء على البيانات المخزنة او المنقولة عبر النظم.

ومن اوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية، عندما تكون السرية Confidentiality والتكاملية أي السلامة Integrity . والقدرة أو التوفر Availability هي التي يتم الاعتداء عليها، بمعنى ان توجه هجمات الكمبيوتر الى معلومات الكمبيوتر او خدماته بقصد المساس بالسرية او المساس بالسلامة والمحتوى والتكاملية، او تعطيل القدرة والكفاءة للانظمة للقيام باعمالها، وهدف هذا النمط الاجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون تخويل ودون ان يدفع الشخص مقابل الاستخدام (سرقة خدمات الكمبيوتر، او وقت الكمبيوتر) او المساس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر وغالبية هذه الأفعال الجرمية تتضمن ابتداءا الدخول غير المصرح به الى النظام الهدف Unauthorized Access والتي توصف بشكل شائع في هذه الايام بأنشطة الهاكرز كناية عن فعل الاختراق[1] Hacking.

والافعال التي تتضمن سرقة للمعلومات تتخذ اشكال عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء، فالكمبيوترات مخازن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق وغيرها وهذه تمثل هدفا للعديد من الجهات بما فيها ايضا جهات التحقيق الجنائي والمنظمات الارهابية وجهات المخابرات والاجهزة الامنية وغيرها، ولا يتوقف نشاط الاختراق على الملفات والانظمة غير الحكومية بل يمتد الى الانظمة الخاصة التي تتضمن بيانات قيمة.

1- منانى فراح: **أدلة الإثبات الحديثة فى القانون**. ص209
.http://www.arablaw.org/Download/CyberCrimes_WorkPaper.doc
(مصدر) تاريخ الدخول 2011/3/16

فعلى سبيل المثال:

قد يتوصل احد المخترقين للدخول الى نظام الحجز في احد الفنادق لسرقة ارقام بطاقات الائتمان. وتتضمن بعض طوائف هذا النمط أي الكمبيوتر كهدف انشطة سرقة والاعتداء على الملكية الفكرية كسرقة الاسرار التجارية واعادة انتاج ونسخ المصنفات المحمية وتحديدا برامج الحاسوب. وفي حالات اخرى فان افعال الاختراق التي تستهدف انظمة المعلومات الخاصة تستهدف منافع تجارية او ارضاء اطماع شخصية كما ان الهدف في هذه الطائفة يتضمن انظمة سجلات طبية وانظمة الهاتف وسجلاته ونماذج تعبئة البيانات للمستهلكين وغيرها.

ب- وقد يكون الكمبيوتر اداة الجريمة لارتكاب جرائم تقليدية

A Tool In The Commission Of A Traditional Offense

كما في حالة استغلال الكمبيوتر للاستيلاء على الأموال باجراء تحويلات غير مشروعة او استخدام التقنية في عمليات التزييف والتزوير، او استخدام التقنية في الاستيلاء على ارقام بطاقات ائتمان واعادة استخدامها والاستيلاء على الاموال بواسطة ذلك، حتى ان الكمبيوتر كوسيلة قد يستخدم في جرائم القتل، كما في الدخول الى قواعد البيانات الصحية والعلاجية وتحويرها او تحوير عمل الاجهزة الطبية والمخبرية عبر التلاعب ببرمجياتها، او كما في اتباع الوسائل الالكترونية للتأثير على عمل برمجيات التحكم في الطائرة او السفينة بشكل يؤدي الى تدميرها وقتل ركابها.

جـ- وقد يكون الكمبيوتر بيئة الجريمة:

وذلك كما في تخزين البرامج المقرصنة فيه او في حالة استخدامه لنشر المواد غير القانونية او استخدامه اداة تخزين او اتصال لصفقات ترويج المخدرات وانشطة الشبكات الاباحية ونحوها.

وطبعا يمكن للكمبيوتر ان يلعب الادوار الثلاثة معا، ومثال ذلك ان يستخدم احد مخترقي الكمبيوتر (هاكرز) جهازه للتوصل دون تصريح الى نظام مزود خدمات انترنت (مثل نظام شركة امريكا اون لاين) ومن ثم يستخدم الدخول غير القانوني

لتوزيع برنامج مخزن في نظامه (أي نظام المخترق) فهو قد ارتكب فعلا موجها نحو الكمبيوتر بوصفه هدفا (الدخول غير المصرح به) ثم استخدم الكمبيوتر لنشاط جرمي تقليدي (عرض وتوزيع المصنفات المقرصنة) واستخدم كمبيوتره كبيئة او مخزن للجريمة عندما قام بتوزيع برنامج مخزن في نظامه.

اما من حيث دور الكمبيوتر في اكتشاف الجريمة، فان الكمبيوتر يستخدم الان على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم، عوضا عن ان جهات تنفيذ القانون تعتمد على النظم التقنية في ادارة المهام من خلال بناء قواعد البيانات ضمن جهاز ادارة العدالة والتطبيق القانوني، ومع تزايد نطاق جرائم الكمبيوتر، واعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة، فانه اصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها، من هنا يلعب الكمبيوتر ذاته دورا رئيسا في كشف جرائم الكمبيوتر وتتبع فاعليها بل وابطال اثر الهجمات التدميرية لمخترقي النظم وتحديدا هجمات الفيروسات وإنكار الخدمة وقرصنة البرمجيات[1].

1- يونس عزب:" **جرائم الكمبيوتر والإنترنت**" (أبوظبى: المركز العربى للدراسات والبحوث الجنائية) **مؤتمر الأمن العربى** ص20،19.

حادى عشر: المعوقات التى تمنع توقيع العقاب على مرتكبى جرائم الإنترنت.

أ- قلة التشريعات التى تواجه جرائم الكمبيوتر، بحيث نجد أفعالا إجرامية لا ينطبق عليها أى نص فى قانون العقوبات.

ب- جرائم الكمبيوتر ذات بعد دولى فيمكن أن يرتكب الجريمة شخص فى خارج القطر المصرى وتقع النتيجة فى مصر، ونظرا لوجود ذلك البعد الدولى يثار تساؤل حول امكانية توقيع العقاب على المجرم فى الخارج.

جـ- لا يوجد لدى المشرعين القانونين والقضاة الخبرة الكافية للتعامل مع الكمبيوتر.

د- فى كثير من الأحيان لا يعرف المجنى عليه أنه أصيب بفيروس، وذلك لوجود فيروسات تظل كامنة فترة طويلة حتى تنشط فى أثارها التدميرية، وحتى لو عرف المجنى عليه بإصابة جهازه بالفيروس، فهناك صعوبة فى معرفة الفاعل وتتبعه ملاحقته جنائيا.

هـ- أحيانا تكون الأثار الناجمة عن الفيروس غير مادية وبالتالى يصعب تقديرها كإتلاف برنامج أو مسح معلومات.

و- فى كثير من الأحيان ويفضل المجنى عليه خاصة إذا كان مؤسسة مالية كبيرة كالبنوك، وعدم التبليغ عن الاصابة بالفيروس حتى لا تهتز ثقة المتعاملين[1].

وبما أن هناك جرائم إلكترونية ترتكب ومجرم يرتكب الجريمة فلابد من وجود ضحايا لهذه الجرائم. وفيما يلى عرض لضحايا الجرائم الإلكترونية

1- محمد أمين الروس: **"جرائم الكمبيوتر والإنترنت"**، (الأسكندرية : دار المطبوعات الجامعية، 2004) ص30،31.

ثاني عشر: ضحايا الجرائم الإلكترونية.

بعد الارتفاع المتزايد في مستخدمي الإنترنت في المملكة بشكل خاص والمنطقة العربية بشكل عام تزايدت التهديدات الأمنية في مجال المعلوماتية خلال الفترة الماضية، ويعد معدل النمو في استخدام الإنترنت في منطقة الشرق الأوسط خلال الفترة من 2000 – 2011 ثاني أعلى معدل إقليمي على مستوى العالم، حيث يصل عدد مستخدمي الإنترنت في الخليج إلى ما يقارب 4 ملايين مستخدم، بمعدل انتشار للإنترنت يساوي 10.%.

وكشف تقرير حديث حول الجرائم الإلكترونية إلى وقوع 65% من البالغين في جميع أنحاء العالم ضحية جرائم الإنترنت، كان ذلك في تقرير لشركة سايمنتك المتخصصة بإصدار البرامج الأمنية، أما تقرير شركة نورتن فقد أشار إلى أن حجم الخسائر الناتجة من هذه الهجمات يصل إلى 114 مليار دولار سنوياً، مما يوضح خطورة وتعقيد أساليب الجريمة الإلكترونية.

وتشير التقارير أيضاً إلى أن ثلثي البالغين الذين يقضون أوقاتهم على الإنترنت قد وقعوا ضحايا لجرائم الإنترنت، ويكثف المجرمون الإلكترونيون نشاطهم على مدار اليوم، إذ تشير التقارير إلى وقوع ضحيتين كل دقيقة.

ويغلب على مستخدمي الإنترنت في الخليج ندرة المعرفة الأمنية وعدم إدراك خطورة المهارات العالية والقدرات المتطورة لمرتكبي الجرائم الرقمية، وعدم الإلمام بنوعيات برمجيات الأمن التي من الممكن الاستفادة منها لتحقيق السلامة الإلكترونية.

ومن الأفضل أن يتسلح مستخدمو الإنترنت في المنطقة بالمعارف والمهارات الرئيسية المتعلقة بالأمن الإلكتروني والخصوصية وكيفية حماية أنفسهم من الأنشطة الإجرامية عبر الإنترنت[1].

1 -http://www.alriyadh.com/2012/03/31/article723214.html
(مصدر) تاريخ الدخول 2012/4/14 الساعة 2 صباحا.

هذا بالإضافة إلى ما كشفت عنه دراسة حديثة صادرة عن مؤسسة سايمنتك أن الشباب هم الفئة الأكثر عرضة للوقوع ضحايا الجرائم الإلكترونية, والتي تنافس في تكلفتها السنوية تجارة العقاقير غير القانونية عبر العالم.

وقدر تقرير صدر هذا العام 2011م عن سيمانتك أن التكلفة السنوية للجرائم الالكترونية تقدر بمبلغ 3888 مليار دولار, منها 114 مليار دولار تعتبر اختلاسا مباشرا و274 مليار دولار تشمل الوقت المهدر نتيجة هذه الجرائم.

وأوضحت الدراسة أنه بشكل عام هناك 589 مليون شخص تأثروا بالجرائم الإلكترونية منهم 431 مليون شخص في العام الماضي فقط, وذلك حسب الدراسة التي شملت 24 دولة وضمت 19636 شخصا خضعوا للدراسة.

وبينت الدراسة أن المتاجرة بالمخدرات قدرت بمبلغ 411 مليار دولار على مستوى العالم، والجرائم الالكترونية فاقت هذا الرقم من المتاجرة في السوق السوداء التي بلغت من بيع المرجوانا والكوكايين وحدهما 288 مليار دولار.

وكانت معظم الجرائم على شكل فيروسات وجرائم خبيثة والتي مارسها 54% منهم, بينما قام 11% بالنصب عن طريق الإنترنت و10% التوصل لمعلومات حساسة مثل كلمة السر أو الدخول لحسابات العملاء, وبالنسبة لجرائم الهواتف النقالة وجدت الدراسة أن 10% وقعوا ضحاياعن طريق خدمة الرسائل القصيرة للاستيلاء على أرقام حساسة للعملاء مثل كلمات السر أوالحسابات.

وأكدت الدراسة التي شملت 24 دولة, أن مليون شخص يوميا يقعون ضحايا الجرائم الالكترونية, كما أن معدل الساعات التي يقضوها على الانترنت تتناسب طرديا مع معد لاستهدافهم مع عصابات الجرائم الالكترونية, فالذين يقضون (49) ساعة أسبوعيا في تصفح النت, يكون (79%) منهم معرض للوقوع في فخ عصابات النت, والذين يقضون 24 ساعة أسبوعيا أو أقل كانت نسبة وقوعهم ضحايا (64.%)

وكانت نسبة وقوع الضحايا بالنسبة لأعمارهم (75%) لجيل الألفية الذي أعمارهم حول العشرسنوات و(61%) للذين أعمارهم بين العشرين والثلاثين, و(80%) للمراهقين, و(75%) للبالغين.

وهذه الأرقام العالية تمثل ثلاثة أضعاف ضحايا الجرائم الجسدية، ورغم ذلك لاحظتالدراسة أن (70%) من الذين خضعوا للدراسة أنهم يكونوا أكثر أمنا على النت أكثر منواقعهم اليومي في الأشهر 12 القادمة.

واختتمت الدراسة بالتذكير أن بعض المشاكل يمكن تجنبها حيث أن (41%) من الشبابلم يقوموا بتحديث الضرورات الأمنية لمواقعهم[1].

إلا أن الغالية العظمى من ضحايا الجرائم الإلكترونية إلى الحفاظ على سمعتهم التجارية ومكانتهم المرموقة، الأمر الذى يؤدى إلى عدم تقديم نطاق أفعال الغش المعلوماتى بسبب ردود الأفعال السلبية لضحايا هذه الأفعال ويبقى صمت وسلبية هؤلاء الضحايا خير معين لمرتكبى هذه الأفعال مما يؤدى فى نهاية الأمر إلى ارتفاع الرقم الأسود لجرائم الحاسب الألى.

ومردود ذلك.

أ- قلة عدد الجرائم الإلكترونية التى يتم التبليغ عن وقوعها لمساسها فى أغلب الأحيان بسمعة المجنى عليهم.

ب- قلة جرائم الحاسب الألى التى يمكن اكتشافها نظرا لما تنطوى عليه هذه الجرائم من تعقيد فى أساليب ارتكابها[2].

1- جريدة الرياض الإقتصادى العدد 15823 يوم الخميس 2011/10/20.

2- عبد الله حسين على محمود: **"سرقة المعلومات المخزنة فى الحاسب الألى"**، ط1 (القاهرة: دار النهضة العربية،2001) ص79،80.

وتتمثل ضحايا الجرائم الإلكترونية فى القطاعات الأتية:

أ- الدول:

مثل سرقة المعلومات العسكرية والمشروعات العامة والمشروعات النووية والتصنيع الحديث للأسلحة المتطورة، وكل ما يمس الأمن القومى لهذه الدول.

ب- سرقة المعلومات المالية

فيما يتعلق بالمراكز الإدارية والمالية الاستثمارات فى المنشأت العامة والخاصة.

جـ- المؤسسات التجارية:

وتتمثل فى الدراسات الخاصة بالأسواق من حيث جدوى المشروعات الراهنة، وكذلك المشروعات الاستثمارية والإنتاج والتجارة والتوزيع.

د- البنوك:

وهى اكثر القطاعات استهدافا ويتباين رد فعل الضحايا بين الصمت وعدم الكشف عن أنهم وقعوا ضحايا للحفاظ على سمعتهم التجارية ومكانتهم المرموقة[1].

ونظرا لوجود الجرائم الإلكترونية والتى تتسبب فى كثير من الخسائر سواء على مستوى الأفراد أو الكيانات الاقتصادية والمؤسسات والدول فلابد من توافر سبل لمكافحة هذا النوع من الجرائم.

1- محمد على العريان: "**الجرائم المعلوماتية** "،(الأسكندرية: دار الجامعة الجديدة للنشر،2004) ص67،68.

ثالث عشر: أساليب مكافحة الجرائم الإلكترونية.

لما كان عصر توظيف المعلومات والاتصالات الذى نعيشه الأن قد أفرز الانترنت التى تثير بدورها الكثير من القضايا مثل قضايا حقوق النشر والتجارة الإلكترونية، فقد كان لابد من وضع قواعد لتنظيم علاقات مستخدمى هذه الأداة التكنولوجية وتحديد حقوق وواجبات كل منهم تجاه الأخر.

والواقع أن أشكال التكنولوجيا تخلق مجالات ثقافية جديدة. وكان من الطبيعى أن تتكيف التشريعات القانونية مع هذه الأشكال الثقافية المستحدثة[1]، فلولا ظهور السيارة ما ظهرت قوانين المرور لذلك ظهور الإنترنت أدى إلى ظهور الجرائم الإلكترونية فكان من الضرورى ظهور قوانين لمكافحة هذا النوع من الجرائم.

ولكن ما يجدر الإشارة إليه أن مكافحة الجرائم الإلكترونية لن يكون له أى تأثير يذكر إلا إذا كان هناك تعاونا دوليا على أكبر قدر من التنسيق والتعاون وعليه يمكننا القول أن أى مجهود أو اجراءات قد تقوم بها أى من الدول على مستوى العالم لن يأتى بأى نتائج ملموسة تحد من إرتكاب تلك النوعية من الجرائم.

فهذه الجرائم لها طابع خاص تتسم به هو أنها جرائم عابرة الحدود، فهى لا تتم من داخل دولة ويكون تأثيرها منحصر فى تلك الدولة، وإنما تلك الجرائم ترتكب عبر عدد من الدول لتتم فى دولة أخرى وتكون أثارها ممتدة لتصل إلى عدد غير محدود من الدول.

وعليه فإن الأساس الذى يرتكز عليه مجال مكافحة الجرائم الإلكترونية هو التعاون الدولى وتنسيق الجهود المبذولة بين كافة دول العالم؛ لتكون هناك نتائج مهمة يمكن الارتكاز عليها وتقويتها للحد من تلك الجرائم ذات النتائج البشعة على اقتصاديات الدول والكيانات الاقتصادية.

1- بهاء شاهين: **"الإنترنت والعولمة"**، ط1(القاهرة:عالم الكتب،1999) ص59.

وعليه فسوف يكون التعاون المشترك بين الدول لمكافحة الجرائم الإلكترونية من خلال التركيز على التعاون الدولى والعناصر التى يرتكز عليها هذا التعاون والتى تنحصر فى الأتى:

أ- المعاهدات والمؤتمرات الدوليه.

ب- إصدار قوانين جديدة:

تجرم الجرائم الإلكترونية فى كافة أنحاء العالم بحيث يكون بينها قدر كبير من التناسق.

جـ- اتحاد الشركات والكيانات الاقتصادية الكبرى فى مجال حماية أمنها الإلكترونى[1].

د- التعاون الدولى.

على صعيد التعاون الدولى فهناك جهود تبذل ليس على مستوى إقليم بعينه ولا على مستوى دولة بعينها وإنما على المستوى الدولى وذلك من خلال الإهتمام بالمؤتمرات الدوليه بجرائم الحاسب الألى، وان كان يدل ذلك على شىء فيدل على خطورة تلك الجرائم وجسامة الأضرار التى تعانى منها الدول.

وقد يتبادر إلى أذهان البعض أن اهتمام المؤتمرات الدولية بالجريمة ليس بالأمر الجديد، بل أن هناك مؤتمرات دوليه تعقد لهذا الشأن فما وجه الغرابة فى ذلك، ولكن الجديد هو أن نجد مؤتمرات تهتم بطائفة من الجرائم وتخرج بتوصيات محددة ويطلب من الدول على إثرها تجريم أنشطة بعينها وهذا هو الجديد[2].

1- منير محمد الجهينى، ممدوح محمد الجهينى:**"جرائم الإنترنت والحاسب الألى ووسائل مكافحته"**، مرجع سابق ص95.

2- محمد حماد الهيتى: **"جرائم الحاسوب"**، ط1(عمان: دار المناهج، 2006) ص163.

هـ- إصدار تشريعات ضد جرائم النت

تعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها.

وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (1976م - 1985م)، وفي عام (1985م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (1986م) صدر قانونا تشريعاً يحمل الرقم (1213) عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (1981م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى.

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت في عام (1985م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي.

وفي عام (1985م) سنّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو

لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها.

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988م) القانون رقم (19-88) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها.

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام.

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته.

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج.

وعلى مستوى الدول العربية لم تقم أي دولة عربية بسن قوانين خاصة بجرائم الحاسب الآلي والانترنت.

ففي مصر مثلا:

لا يوجد نظام قانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية.

وكذا الحال بالنسبة لمملكة البحرين:

فلا توجد قوانين خاصة بجرائم الإنترنت، وان وجد نص قريب من الفعل المرتكب فان العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة على جريمة الإنترنت.

وفى السعودية:

أعلنت السلطات المختصة أنها ستفرض عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال فيما يعادل 133 ألف دولار لجرائم القرصنة المرتبطة بالانترنت واساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور دون تصريح[1].

الجهود الدولية المبذولة لمواجهة الجرائم الإلكترونية.

مع تزايد الخسائر الناجمة عن جرائم الحاسب الألى وتزايد حجم الأضرار الناشئة عنها والتى تتخطى فى أغلب الأحيان حود الدول لتطال أجهزة الحاسب الألى المملوكة إلى الأفراد وإلى المؤسسات المالية والحكومات بات أمر التعاون الدولى لمواجهتها ضرورة حتمية.

وتبذل الأمم المتحدة جهودا لايستهان بها فى مجال محاولة التصدى لجرائم الحاسب الألى للحد من انتشارها وتعاظم أثارها.

وتبنى مؤتمر هافانا بعض التوصيات التى خرج بها مؤتمر الأمم المتحدة السابع عام 1985 وأدخل عليها بعض التعديلات

1- http://www.moheet.com 2010/12/21 تاريخ الدخول (مصدر)

ويمكن إجمال توصيات مؤتمر هافانا عام 1990 فى المبادىء التالية[1].

أ- تحديث القوانين الجنائية الوطنية بما فى ذلك التدابير المؤسسية.

ب- تحسين أمن الحاسب الألى والتدابير المعنية.

جـ- اعتماد إجراءات تدريب كافية للموظفين والوكالات المسؤلة عن منع الجرائم الإقتصادية والجرائم المتعلقة بالحاسب الألى والتحرى والإدعاء فيها.

د- تلقين أداب الحاسب الألى كجزء من مقرارات الاتصالات والمعلومات.

هـ- اعتماد سياسات تعالج المشكلات المتعلقة بالمجنى عليهم فى تلك الجرائم.

و- زيادة التعاون الدولى من أجل مكافحة هذه الجرائم.

وحتى عام 2000 عقدت الأمم المتحدة مؤتمرها العاشر لمنع الجريمة ومعاملة المجرمين فى بودابست بالمجر وأكدت على وجوب العمل الجاد للحد من جرائم الحاسب الألى[2].

وما يجدر الاشارة إلية أنه يجب أن نسير على المبدأ القائل بأن الوقاية خيرا من العلاج بمعنى أنه لابد من حماية شبكة الانترنت من الاختراق بدلا من تركها ليصبح مستخدميها عرضة للجرائم الإلكترونية على شتى أنواعها **لذلك سنتطرق إلى:**

1- محمود أبو عبابنة:" **جرائم الحاسوب وأبعادها الدولية**"، (عمان: دار الثقافة،2005) ص152.
2- حمد أمين أحمد: "**جرائم الحاسوب والإنترنت –الجريمة المعلوماتية**"، (عمان: دار الثقافة،2004) ص74.

رابع عشر: سبل الأمان والحماية على الإنترنت.

1- فهم طبيعة المخاطر التى قد يتعرض لها نظام تبادل المعلومات فى الشبكة ونتائج هذه المخاطر.

2- عمل سياسة أمنية متعددة المستويات، بحيث يمكن تنظيم ومواجهة الأخطار العملية العالية التعقيد التى ترافق أى نظام معلوماتى.

3- اعتماد الشبكة على نظام امنى يوفر حماية المعلومات من أخطار الاختراق بحيث تكون المهمة الأساسية لنظام الحماية تكون فى عزل نظام المعلومات فى الشبكة عن مصادر الخطر المتعددة التى تؤدى إلى تسريب المعلومات السرية[1].

وتتمثل أشكال الحماية فى الأتى:

أ- حماية وأمن الشركات على الإنترنت.

إن أكثر الطرق شيوعا لحماية لحماية المعلومات السرية والحساسة فى شبكة الشركة أو المؤسسة هى بناء جدار حماية (Fire Wall) بين شبكة الشركة والانترنت مما ينشىء حيز بينهما، وذلك عن طريق تخصيص جهاز حاسوب واحد تمر منه المعلوملت القدمة إلى الشركة والخارجة منها لتقييمها وتحليلها ليرى إذا كانت تخرق قواعد الحماية أم لا.

ب- التنقل الأمن على الإنترنت:

يعتبر الكثير من مواقع الويب التجارية غير أمنة وتتزايد بشكل مستمر ولكن بإمكانك الأن القيام بعدة معاملات تجارية أمنة على الويب وتنفيذ بعض عمليات التسوق فعناوين صفحات الويب غير الأمنه تبدأ بـ //:http إضافة لذلك يعرض

1- حسام ملحم، عمار خير بك: **"شبكات الانترنت بنيتها الأساسية وانعكاساتها على المؤسسات"، ط 1 (دار الرضا، 2000) ص 118.**

برنامج Netscape صورة مفتاح مكسور مشيرا بذلك إلى أن صفحة الويب غير أمنة، بينما عنوان الصفحة الأمنة فيبدأ بـ //:https إضافة لذلك يعرض برنامج Netscape رسالة يعلمك فيها بأن المعلومات التى سترسلها سيتم تشفيرها وعند وصولك إلى صفحة أمنه يعرض برنامج Netscape صورة لمفتاح غير مكسور على خلفية زرقاء.

جـ- حماية الأطفال على الإنترنت.

إذا كنت مشتركا بالانترنت فى المنزل أو فى المدرسة فلا شك أنك تريد أن يحصل أبنائك على خبرة إيجابية بناءة عند تصفحم لصفحات الويب ويمكن حمايتهم من خلال استخدام برنامج Cyber Patrol وهو برنامج مزودة بقائمة المواقع الممنوعة والتى تحوى عنف ومواد إباحية وغيرها أو برنامج Surf Watch ويمكن تنزيلها على الجهاز أو استخدام الموقع Bess الذى يوجه الأطفال نحو المناطق المخصصة لهم.

د- حماية الحاسوب من الفيروسات.

الفيرس هو برنامج وسمى بالفيرس لأنه يشبه تأثير الفيرس فهو يتكاثر وينتقل من حاسوب إلى أخر وهناك طرق عدة للوقاية منه.

- عدم استخدام أقراص مرنه من أشخاص أخرين.
- أخذ نسخة إحتياطية من من قرصك الثابت.
- استخدام برنامجى Virus-Scan& Norton Antiviruse وذلك لكشف الفيروسات[1].

1- زياد القاضى، قضى القاضى وأخرون: **"مقدمة إلى الانترنت"**، ط 1(عمان: دار صفاء للنشر والتوزيع،2000) ص213- 216.

الفصل الثانى

الإرهاب الإلكترونى

أسبابه ومخاطره وطرق مكافحته

أولاً: تعريف الارهاب الإلكترونى.

ثانياً: أسباب الارهاب الإلكترونى.

ثالثاً: أشكال الإرهاب الإلكترونى.

رابعاً: خصائص شبكة الانترنت الجاذبة للتنظيمات الإرهابية.

خامساً: مخاطر استخدام شبكات الأنترنت.

سادساً: مظاهر الإرهاب الإلكترونى.

سابعاً: أهداف الشبكات (المواقع) الإرهابية.

ثامناً: وسائل الإرهاب الإلكتروني.

تاسعاً: أبعاد وسمات أعضاء التنظيمات الإرهابية على الإنترنت.

عاشراً: دور رأس المال الاجتماعي فى دعم الإرهاب الإلكترونى.

حادى عشر: مراحل تكوين العناصر المتطرفة على الإنترنت.

ثانى عشر: منهج التنظيمات الإرهابية فى السيطرة على عقول الشباب.

ثالث عشر: مدارس الخطاب الفكري الإسلامي على الشبكة العنكبوتية.

رابع عشر: توظيف مواقع التواصل الاجتماعى فى خدمة الارهاب ومكافحته.

خامس عشر: العلاقة بين الاعلام والارهاب.

سادس عشر: طرق مكافحة الارهاب الالكترونى.

سابع عشر: استراتيجيات الوقاية من الإرهاب الالكترونى.

ثامن عشر: الجهود الدولية لمكافحة الارهاب الإلكترونى.

تاسع عشر: صعوبة اكتشاف جرائم الإرهاب الإلكتروني.

مقدمه

بداية خلق الله كان الإنسان البدائى الذى كان يتعامل مع الطبيعة فى صورتها البدائية حيث لم يكن هناك أى تطور فى البيئة المحيطة به، ولكن الانسان نفسه هو من طور بيئته وفقا لإحتياجاته، فبعد أن عرف النار عن طريق احتكاك الأحجار مع بعضها البعض لتوليد شرارة النار أصبح الأن يستخدم البوتاجاز بالكهرباء وهذا بفعل التطور التكنولوجي الهائل الذى أصبحنا فيه الأن.

كذلك الإرهاب بدأ فى صورته البدائيه بالقتل ثم مع اختراع الديناميت على يد ألفريد نوبل استخدمه الانسان وتطور لأكثر من ذلك إلى القنابل والصواريخ والأسلحة المتطورةّ، ثم استخدام التكنولوجيا الناعمة فى القتل والإرهاب وهذا هو موضوعنا فى هذا الفصل حيث تم استغلال التطور التكنولوجي متمثلا فى الإنترنت والمحمول فى الإرهاب تحت مظلة ما يسمى بالإرهاب الإلكترونى.

أولاً: تعريف الإرهاب الإلكتروني:

تعددت التعريفات التى تناولت الإرهاب الالكترونى منها على سبيل المثال وليس الحصر.

أنه استخدام وسائل إلكترونيّة في عدوان أو تخويف أو تهديد له طابع مادي أو معنوي، ويصدر من دول أو جماعات أو أفراد عبر الفضاء الإلكتروني. كما يعني أن يسعى ذلك العدوان للتأثير على الاستخدام السلمي للفضاء الإلكترونى.

كما يمكن تعريف "الإرهاب الإلكتروني"، حتى نكون أكثر وضوحاً ودقة بأنه "نشاط أو هجوم متعمّد، يملك دوافع سياسية ويسعى للتأثير في القرارات الحكومية والرأي العام العالمي، ويستخدم الفضاء الإلكتروني بوصفه عاملاً مساعداً ووسيطاً في عملية التنفيذ للعمل الإرهابي، أو الحربي. كما يسعى لإحداث تأثير معنوي ونفسي عبر التحريض على بث الكراهية الدينية وحروب الأفكار. ويأتي هذا العمل في صورة رقميّة عبر استخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور في الفضاء الإلكتروني، وقد يقتصر تأثيرها على بعدها الرقمي، أو تتعداه لتصل إلى الإضرار بأهداف مادية تتعلق بالبنية التحتية الحيويّة"[1].

فى حين يرى البعض الإرهاب الالكترونى:

أنه استخدام التقنيات الرقمية لإخافة واخضاع الأخرين، أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو اقتصادية أو أمنية أو عرقية أو دينية، أى أنه توظيف لأحدث التقنيات العلمية فى الضغط والتوجيه والسيطرة على الأخرين أيا كانوا أفرادا أو مؤسسات أو دول وأنظمة وكيانات سياسية أو أقتصادية أو حتى تكنولوجية وبهدف كسر ارادة هذا الأخر للتمكن منه[2].

ويأتي الإرهاب الإلكتروني أيضاً في صورة القيام بهجوم طبيعي، عن طريق استخدام الأسلحة التقليدية في مهاجمة كابلات الاتصال ونقاط الإنترنت الرئيسية

1- تايم لاين جريدة الرياض، العدد 17202، الخميس 14 شوال 1436 هـ - 30 يوليو 2015م.

2- سعد عطوة الزنط: الارهاب الالكترونى واعادة صياغة استراتيجيات الأمن القومى، **مؤتمر الجرائم المستحدثة كيفية اثباتها ومواجهتها** (المركز القومى للبحوث الاجتماعية والجنائية،2010).

ومحطات البث. وينطبق التعريف نفسه على استخدام الطاقة الكهرومغناطيسية في مهاجمة أجهزة الكومبيوتر أو البيانات التي تحويها، بما يؤثر في عملها. ويشمل التعريف عينه، شنّ هجمات تستخدم أسلحة الفضاء الإلكتروني المتنوّعة بهدف إلحاق الضرر بمصالح المجتمع الدولي.

هذا فى ظل عدم وجود اتفاق دوليّ واضح في التعامل مع ظاهرة الفضاء الإلكتروني وتنظيم استخدامها وتحديد الحقوق والواجبات، مما يجعل الدول لا تشعر بأي إلزام في التعاون مع غيرها. ويلاحظ أن عدم التعاون بين الدول يشكّل جزءاً مهمّاً من تعقّد المشكلة، مما يؤثر في معرفة الهجمات الإلكترونيّة ومواجهتها، إذ يتمثّل هدف التعاون في حماية السيادة والأمن والمصالح الأساسيّة المشتركة. كما أن تعرّض الدول لهجمات الشبكات وقواعد البيانات، يمثل تهديداً لمصالحها الوطنيّة ويؤثر في تطوّرها تكنولوجيّاً، وفي مساعيها لحماية أمنها وخصوصية مواطنيها.

وتشكّل القواعد القانونية ضغطاً دبلوماسياً على الدول التي لا تدرك أو تعترف بأن الإرهاب الإلكتروني يعتبر جريمة دولية. وبقول آخر، يمهّد الضغط الدبلوماسي الطريق أمام تعزيز الرؤى حول خطورة استخدام الهجمات الإلكترونيّة في الصراعات، ما يحتّم نمطاً جديداً من التعاون بين الدُوَل.

خلاصة القول:

أن هجمات الإرهاب الإلكتروني هي نوع من ممارسة القوّة في العلاقات الدوليّة. ويشير إلى إمكان استخدام تلك الهجمات في ضرب مراكز التحكّم والسيطرة، والهجوم على شبكات الطاقة وأنظمة التسلّح. وينتج من تلك الهجمات تدمير مادي وآثار تدميرية تشبه ما ينتج من استخدام أسلحة تقليدية وغير تقليدية، إضافة إلى الآثار الواسعة التي تترتب على هجمات الفضاء الإلكتروني ماديّاً ونفسيّاً[1].

وفى ظل انتشار الإرهاب فى مجتمعاتنا العربية والذى أصبح يهدد وجودها وبقاءها كان من الضرورى بما كان البحث فى أسباب الإرهاب الإلكترونى ودوافع إرتكابه **والتى يمكن رصدها فيما يلى:**

1- الإرهاب الإلكتروني والقوّة في العلاقات الدولية تاريخ الدخول الثلاثاء 2016/6/28
http://www.alhayat.com/Articles /

ثانياً: أسباب الإرهاب الإلكتروني ودوافعه:

إن أسباب الإرهاب الإلكتروني ودوافعه متعددة ومتنوعة، وهي عينها أسباب ظاهرة الإرهاب عموماً؛ وذلك لأن الإرهاب الإلكتروني يعتبر نوعاً من أنواع الإرهاب وشكلاً من أشكاله, كما أن هناك عوامل عديدة تجعل من ظاهرة الإرهاب الإلكتروني موضوعاً مناسباً وسلاحاً سهلاً للجماعات والمنظمات الإرهابية, وبالنظرة الشاملة المتوازنة يمكننا القول بأن الأسباب متشابكة والدوافع متداخلة, حيث تتداخل الدوافع الشخصية مع الفكرية والسياسية والاقتصادية والاجتماعية, فالظاهرة التي نحن بصددها ظاهرة مركبة معقدة, وأسبابها كثيرة ومتداخلة, وسوف نتطرق في هذا الفصل إلى بيان الأسباب العامة للإرهاب الإلكترونى و دوافع انتشاره، وكذلك الأسباب الخاصة بشبكة الانترنت والتى ساهمت بدورها فى انتشار الإرهاب الإلكترونى.

أ- وتتمثل الأسباب العامة للإرهاب الإلكترونى فى:

1- البطالة وقلة فرص التعليم

والتهميش وضعف المشاركة في الحياة العامة. وللتخطيط للمستقبل ينبغي أن نعرف أن أكثر من 50% من سكان العالم العربي تحت سن 15 سنة، وتأسيسًا على ذلك فإن مثل هذه الشرائح تعد المستهدف الرئيس بثقافة التطرف والعنف خاصة وأن ظروف واقعهم المعيشي والحضاري قد يسمح بتسلل[1]. الأفكار الشاذة والمتطرفة، وقد حددت بعض الدراسات (أربعة أنواع من الحاجات الأساسية التي يحتاجها شباب العالم الاسلامي في عصر العولمة والصراع الحضاري وهي (الحاجة إلى الأمن، الحاجة إلى الهوية، الحاجة إلي الحرية، الحاجة إلى الصحة) وهذا غير متوفر.

1- فايز الشهرى: **ثقافة التطرف والعنف**، مرجع سابق.

2- الفراغ

الذى يعانى منه الكثير من الشباب فى مجتمعاتنا العربية.

3- أن فئة الشباب بحسب كثير من الدراسات هم أكثر الفئات استخداما للإنترنت:

وبات واضحا أنهما الشريحة الأكبر على المشهد الالكتروني في العالم العربي فمن الطبيعي أن يتأثروا بهذه الشبكة ويؤثروا فيه اوبالطبع سيكون هناك مستثمرون لهذه الضوضاءا لفكرية، ومن هؤلاء المستثمرين قادة التيارات الفكرية الذين قاموا ويقومون بجهد كبير لضخ الأفكار والمعتقدات وتشكيل قناعات ملايين الشباب واثقين أن التاثير الثقافي والفكري التراكمي سيكون كبيرا[1].

4- الفقر

5- الجهل

حيث أن بعض المجتمعات العربية تعانى من نسبة أمية عالية، هذا بالاضافة إلى أن التعليم نفسه يعلم الفرد أن يكون شخصا تابعا وليس شخصا مفكرا.

6- قلة الوازع الدينى

القائم على أسس الدين الإسلامى السمح والوسطى بعيدا عن التشدد والتطرف، والتأويل الخاطئ لنصوص القرأن والسنة[2].

1- رولا الحمصى: ادمان الانترنت عند الشباب وعلاقته بمهارات التواصل الاجتماعى دراسة ميدانية، **مؤتمر ملتقى الطلاب الإبداعى الثانى عشر**، جامعة أسيوط.

2- الباحثة.

ب- أسباب الإرهاب الإلكترونى كجريمة ترتكب عبر شبكة الأنترنت.

1- ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق:

إن شبكات المعلومات مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها؛ رغبة في التوسع وتسهيل دخول المستخدمين, وتحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على ثغرات معلوماتية, ويمكن للمنظمات الإرهابية استغلال هذه الثغرات في التسلل إلى البنى المعلوماتية التحتية, وممارسة العمليات التخريبية والإرهابية .

2- غياب الحدود الجغرافية وتدني مستوى المخاطرة:

إن غياب الحدود المكانية في الشبكة المعلوماتية بالإضافة إلى عدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة يعدُّ فرصة مناسبة للإرهابيين, حيث يستطيع محترف الحاسوب أن يقدِّم نفسه بالهوية والصفة التي يرغب بها أو يتخفى تحت شخصية وهمية, ومن ثم يشن هجومه الإلكتروني وهو مسترخٍ في منزله من دون مخاطرة مباشرة, وبعيداً عن أعين الناظرين .

3- سهولة الاستخدام وقلة التكلفة:

إن السمة العولمية لشبكات المعلومات تتمثل في كونها وسيلة سهلة الاستخدام, طيعة الانقياد, قليلة التكلفة, لا تستغرق وقتاً ولا جهداً كبيراً, مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة, ومن دون الحاجة إلى مصادر تمويل ضخمة, فالقيام بشن هجومٍ إرهابي إلكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتيةٍ ومزود بالبرامج اللازمة.

4- صعوبة اكتشاف وإثبات الجريمة الإرهابية:

كثير من أنواع الجرائم المعلوماتية لا يعلم بوقوع الجريمة أصلاً وخاصة في مجال جرائم الاختراق, وهذا ما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته, كما أن صعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني؛ لأنها تعطي المجرم أملاً في الإفلات من العقوبة[1].

5- الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية.

إن الفراغ التنظيمي والقانوني لدى بعض المجتمعات العالمية حول الجرائم المعلوماتية والإرهاب الإلكتروني يعتبر من الأسباب الرئيسة في انتشار الإرهاب الإلكتروني, وكذلك لو وجدت قوانين تجريمية متكاملة فإن المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة ثم يقوم بشن هجومه الإرهابي على بلد آخر يوجد به قوانين صارمة, وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق. كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتسيطر على مدخلاتها ومخرجاتها يعدُّ سبباً مهماً في تفشي ظاهرة الإرهاب الإلكتروني, حيث يمكن لأي شخص الدخول ووضع ما يريد على الشبكة, وكل ما تملكه الجهات التي تحاول فرض الرقابة هو المنع من الوصول إلى بعض المواقع المحجوبة, أو إغلاقها وتدميرها بعد نشر المجرم لما يريده فيها.

لكل هذه الأسباب والدوافع أصبح الإرهاب الإلكتروني هو الأسلوب الأمثل والخيار الأسهل للمنظمات والجماعات الإرهابية[2].

1-www.shaimaattalla.com مصدر الخميس 2016/9/15 تاريخ الدخول

2- **عبد الله بن عبد العزيز بن فهد العجلان:** بحث مقدم الى المؤتمر الدولى الاول حول "حمايه أمن المعلومات والخصوصيه فى قانون الانترنت" والمنعقد بالقاهره فى المده من 2 – 4 يونيه 2008م ص30.

وللأسباب السابق ذكرها تتولد لدى الأفراد دوافع لممارسة الإرهاب الإلكترونى ومنها على سبيل المثال:

1- الجانب النفسى.

حيث يقدم الفرد على الإرهاب لأسباب تتعلق بحالته النفسية مثل الضغوط الشديدة التى يتعرض لها من ظروف الحياة.

2- الجانب المادى.

يتمثل بنزوع الأفراد للحصول على مايسد احتياجاتهم ويلبى متطلباتهم المادية وخاصة عندما تتسع الفجوة بين الغنى والفقير، حيث تنجح المنظمات الإرهابية فى استقطابهم مقابل المال.

3- الجانب الوجدانى.

تقوم وسائل الاعلام بطريقة غير مباشرة بتقديم المعلومات عن القضايا التى يعمل من أجلها الإرهابيون مما يؤدى إلى إثارة الأفراد نفسيا،حيث تلقى تلك الحوادث ردود فعل نفسية متباينة قد تكون معارضة لدى البعض ومتعاطفة لدى البعض الأخر،مما يدفعهم للإنضمام للجماعات الإرهابية أو محاولة تقليدها[1].

وما يجدر الاشارة إليه أن الارهاب الإلكترونى مثله مثل غيره من الجرائم له صور **وأشكال متعددة يمكن استعراضها كما يلى.**

1- مخلد خلف النوافعة: **اتجاهات الجمهور الأردنى إزاء قضايا الإرهاب** التى تبثها قناتا الجزيرة والعربية الفضائيتان الإخباريتان (جامعة الشرق الأوسط: كلية الإعلام،2010) ص64.

ثالثاً: أشكال الإرهاب الإلكترونى:

1- ارتكاب جرائم ماسةبسلامة وأمن الدولة سواء من الداخل أو من الخارج بغرض الإرهاب والتخويف وبث الرهبة.

2- إرهاب مستخدمى الحاسب الألى ببث الرهبة والرعب فيهم، أى ارتكاب الجرائم المعلوماتية فى صور تؤدى إلى إثارة الرعب والخوف بين مستخدمى الانترنت سواء بغلق نظم التشغيل، أو إجراء هجوم إلكترونى أو بإزالة المعلومات أو أى صورة تحقق النتيجة المجرمة.

3- اختراق أنظمة المعلومات فى دولة أو مؤسسة كبرى بما يؤدى إلى اضطراب سير العمل و إرباكه.

4- التهديد بإرتكاب جرائم قتل ضد شخصيات سياسية.

5- التهديد بتفجيرات فى أماكن التجمعات والأماكن السياسية ومراكز التجارة والتجمعات الرياضية.

6- القرصنة الإلكترونية بأن تقوم جهات إرهابية بالحصول على المعلومات العسكرية والسياسية المخزنة فى ذاكرة الحاسبات الألية لوزارات الدفاع فى الدول[1].

7- استغلال أجهزة المحمول فى تبادل الرسائل بين أفراد الجماعات الارهابية، والدخول على شبكة الأنترنت وحضور اجتماعات بالصوت والصورة للجماعات المتطرفة لإعطاء الأوامر المطلوب تنفيذها حول العمليات الإرهابية.

1- أحمد على البدرى: الإرهاب الإلكترونى، ورقة عمل المؤتمر الثانى للمركز القومى للبحوث الاجتماعية والجنائية- الجرائم المستحدثة كيفية إثباتها ومواجهتها فى الفترة من 15 - 16 ديسمبر 2016، ص8-9.

8- استغلال أجهزة المحمول الذكية فى التفجيرات عن بعد.

9- استغلال الانترنت فى ارتكاب الجرائم السياسية والاقتصادية حيث تستخدم المجموعات الإرهابية حاليا تقنية المعلومات لتسهيل الأعمال الإجرامية، وهم لا يتوانون عن استخدام الوسائل التكنولوجية المتقدمة مثل بث الأخبار المغلوطة، واستغلال بعض صغار السن،وتحويل بعض الأموال فى سبيل تحقيق أهدافهم حيث يستغل الإرهابيون المؤيديون لأفكارهم، وجمع الأموال لتمويل برامجهم الإرهابية.

10- نشر الصور لبعض الشخصيات العسكرية والتحريض على قتلها وإغتيالها[1].

11- تهديد الأمن القومى عن طريق أساليب التجسس للحصول على المعلومات الهامة ذات الطبيعة السرية[2].

ولعل المتتبع لشبكة الإنترنت يلاحظ أن عدد هذه الشبكات، والتي بلغت 12 شبكة عام 1997، بلغت في أوائل عام 2005 إلى (4,350)، وبحلول عام 2006 بلغت هذه الشبكات (4,800)، وأخيرا تجاوزت أكثر من ستة آلاف شبكة في نهاية عام 2008، حتى وصلت إلى أكثر من 150 ألف موقع فى عام 2016 حيث أصبحت معظم التنظيمات الإرهابية لها وجود علي الإنترنت، وكان لتنظيم القاعدة السبق[3]. فأصبح الانترنت وسيلة اتصالات ومعلومات وتدريب[4].

وقد يرجع ذلك لأن الشبكة أصبحت تتميز بخصائص جعلتها مكانا جاذبا للمتطرفين ومكتبة مفتوحة لنشر الفكر المخالف للسائد في أي مجتمع، **وتتمثل أبرز هذه الخصائص في التالي:**

1- الباحثة.

2- أمير أفونس عريان: الجرائم الإلكترونية فى البنوك - وكيفية مواجهتها (جامعة عين شمس: كلية التجارة، 2010) ص4.

3- رضوى عمار:دور الإعلام فى انتشار ظاهرة الإرهاب، السياسة الدولية،2016/9/1.

4- فايز الشهري: التطرف الالكترونى على شبكة الانترنت رؤية تحليلية، مؤتمر تقنية المعلومات والأمن الوطنى،12-2008/11/ 14.

رابعاً: خصائص شبكة الأنترنت الجاذبة للتنظيمات الإرهابية.

1- أسرع وسائل الاتصال الجماهيري انتشارا وأكثرها تداولا وإقبالا بين الشباب وهم القاعدة العريضة المستهدفة من قبل الجماعات الإرهابية.

2- وسيلة حرة دون حواجز رقابية بين المرسل والمستقبل.

3- تتميز بالخصوصية (السرية) بين المرسل والمستقبل.

4- انتشار المواقع الفكرية لرموز الفكر التكفيري وتواصلها مع زوارها ومعتنقي هذه الأفكار.

5- إن معظم رموز الفكر المتطرف الذين تأثر بهم الشباب لم يعرفوا بشكل جماهيري إلا عن طريق مواقع معينة تروج لفكرهم وتستقطب أتباع الفكر.

6- تشكل المنتديات الحوارية المتطرفة وقود الصراع الفكري للفكر المتطرف مع خصومه.

7- تشكل القوائم البريدية التي يشرف عليها مشرفوا المواقع الالكترونية حلقة الوصل بين معتنقي الأفكار المظللة والأتباع[1].

فقد تطور استخدام الجهاديين للإنترنت بتزايد التواجد على مواقع التواصل الاجتماعي، التي أصبحت أداة لجذب المزيد من المقاتلين. وساعدت هذه المواقع الجماعات الجهادية في تصدير صورة مفادها أن الجهاديين دائما منتصرون، وهذا ما ساعد في تجنيد الشباب وجلب التبرعات.

1- فايز الشهري: التطرف الالكتروني على شبكة الانترنت رؤية تحليلية، مؤتمر تقنية المعلومات والأمن الوطني،12-14 /2008/11.

خامساً: مخاطر استخدام شبكات الأنترنت:

ويمكن ايجازها في النقاط التالية:

1- أن تلك الوسائل الاجتماعية قد أصبحت أداة للجماعات الإرهابية والمتطرفة لنشر الأفكار وتجنيد الأنصار، وبث الصور ولقطات الفيديو والبيانات عن عملياتهم بهدف إثارة الرعب والفزع.

2- التزييف والتشويه للمعلومات من خلال دس المعلومات والأخبار الكاذبة.

3- اختراق الخصوصية من خلال الدخول علي الحسابات الشخصية، والتنصت علي الاتصالات ومن ثم تشويه السمعة واغتيال الشخصيات من خلال اختلاق الأخبار والتلاعب بالصور ولقطات الفيديو ونشر حسابات مزيفة.

4- التجسس وجمع المعلومات عن الأفراد والمؤسسات من خلال الشبكات الاجتماعية وتويتر والواتس أب والفيبر وتهديدهم وابتزازهم.

5- السيطرة والتوجيه وبناء الصداقات المريبة وتجنيد العملاء للتجسس من خلال الشبكات الاجتماعية.

6- نشر الشائعات: المؤثرة علي وحدة وتماسك المجتمع.

7- القرصنة وحرب المعلومات وتخريب أنظمتها: من خلال الاختراق وسرقة البيانات وتدمير نظم المعلومات.

8- التدمير النفسي والاجتماعي للشباب من خلال الإدمان علي الشبكات الاجتماعية والمحمول والمواقع الإباحية والمخدرات الرقمية.

9- الإغتيال والتصفية الجسدية من خلال أدوات تقوم بتحديد الموقع، والتفجير عن بعد عبر الهواتف.

10- التحريض علي العنف والتخريب والقتل[1].

وتزداد هذه المخاطر بإزدياد التعرض لهذه الشبكات واستخدامها والتى تؤدى إلى الإنجراف لإرتكاب بعض الجرائم الإلكترونية ولا سيما الإرهاب الإلكترونى الذى تتجلى مظاهر ارتكابه فى المظاهر الأتية:

1- محمود علم الدين: وسائل التواصل الاجتماعى والأمن القومى وكيف واجهت الدول مخاطر الانترنت والفيسبوك، جريدة أخبار اليوم، العدد 3749، 10 سبتمبر 2016.

سادساً: مظاهر الإرهاب الإلكترونى:

1- نشر رسائل تهديد تثير الرعب وتؤدى إلى استنفار رجال الأمن.

2- إغراق المواقع الهامة للقطاعات الحكومية أو القطاعات الحيوية (DosAttack) مما يسهم فى تعطيلها وشل حركتها وعدم قدرتها على القيام بدورها كما حدث في ثورة الخامس والعشرين من يناير.

3- العمل على تخريب الأنظمة من خلال إرسال الفيروسات والبرامج الخبيثة.

4- التجسس للحصول على المعلومات سواء سياسية أو عسكرية أو تجارية.

5- وسيلة للتواصل بين المجموعات الإرهابية للتنسيق وتلقى المعلومات والخطط والتدريب اللازم بالصوت والصورة.

6- وسيلة إعلامية لبث أخبارهم ونشر أفكارهم وللتحريض على العمليات الارهابية وتبريرها.

7- استقطاب وتجنيد أتباع جدد وخصوصا من صغار السن.

8- توفير التدريب النظرى على العمليات الإرهابية وطرق التفجير.

9- استغلال الإرهابيين لأجهزة الكمبيوتر والإنترنت لنشر معلومات حول كيفية تصنيع القنابل والمتفجرات.

خلاصة القول أن الإرهاب والإنترنت مرتبطان بطريقتين:

الأولى:

أن الإنترنت أصبح منبرا للجماعات والأفراد ... وذلك من اجل رسائل الكراهية والعنف وللاتصال ببعضهم بعضا وبمؤيديهم والمتعاطفين معهم، وشن حروبا نفسية على أعداءهم.

الثانية:

حاول الأفراد والجماعات مهاجمة شبكات الكمبيوتر فيما أصبح يعرف بالإرهاب الإلكتروني أو الحرب الإلكترونية. إلا أن الإرهابيين في هذه المرحلة يستخدمون ويستفيدون من الإنترنت أكثر مما يهاجمونه. فالمواقع الإلكترونية ليست سوى واحدة من خدمات الإنترنت التي سطا عليها الإرهابيون. فهناك تسهيلات عديدة أخرى كالبريد الإلكتروني وغرف المحادثة والمجموعات الإلكترونية والمنابر وألواح الرسائل. ويستخدم الكثير من هذه المواقع الإلكترونية لشن الحملات النفسية ضد الدول المعادية وقواتها المسلحة. فهي تعرض أفلاما مرعبة للرهائن والأسرى أثناء إعدامهم[1]. وليس هذا فقط بل هذه المواقع الإرهابية ذات أهدافا متعددة لا حصر لها منها على سبيل المثال وليس الحصر.

1- 03 ايلول/سبتمبر 32008

http://iipdigital.usembassy.gov/st/arabic/publication/2008

سابعاً: أهداف الشبكات (المواقع) الإرهابية.

تهدف المواقع الإرهابية إلى عدة أهداف منها:

1- نشر الفكر الضال.

2- نشر الإصدارات.

3- جمع الأموال.

4- التجنيد.

5- التدريب[1].

حيث حذَّر مرصد الفتاوى التكفيرية والآراء المتشددة التابع لدار الإفتاء المصرية من تنامي ظاهرة الإرهاب الإلكتروني، التي كانت سببا رئيسيا في انتشار العنف والتطرف، موضحا أن المنتديات الإلكترونية ومواقع التواصل الاجتماعي أضحت الأداة الأهم في يد الجماعات الإرهابية لنشر أفكارها ووضع خططها وتجنيد أعضائها.

وأكد المرصد التكفيري في تقريره الخامس والعشرين والذي جاء تحت عنوان **"دور المنتديات الإلكترونية ومواقع التواصل الاجتماعي في تجنيد الإرهابيين. الخطورة وسبل القضاء عليها"** أن 80% من الذين انتسبوا إلى تنظيم الدولة الإسلامية تم تجنيدهم عبر وسائل التواصل الاجتماعي.

1- عطا الله بن فهد السرححاني: توظيف شبكات التواصل الاجتماعي فى مكافحة الارهاب، دورة تدريبية خلال الفترة من 23-27 /2/2013م.

وقال التقرير إن عدد المواقع الإلكترونية المحسوبة على هذه الجماعات ارتفع من 12 موقعا إلكترونيا عام 1997 ليصل – حسب آخر الإحصائيات – إلى 150 ألف موقع عام 2015.

وأرجع التقرير أسباب استخدام المتطرفين لشبكات التواصل الاجتماعي، إلى قلة عبئها المادي؛ حيث أن الاعتماد على آلية منخفضة التكلفة يتيح نشر المعلومات عن التنظيمات وكيفية التواصل مع أعضائها، بالإضافة إلى إتاحة تدفق المعلومات وتقليل تكلفة تجنيد الأعضاء، وإيجاد مجتمعات للتواصل الإلكتروني يتشارك أعضاؤها الأفكار والنقاش.

وأكد التقرير أنها تساهم في عملية التنسيق بين أعضاء الجماعات، معتبرا موقع تويتر أحد أهم وسائل التواصل التي تستخدم للتفاعل وتنسيق العمليات الإرهابية.

وتكمن الميزة الأساسية في تويتر في أنه يوفر مجتمعات افتراضية متغيرة، تتكون بصورة تلقائية خلال الأحداث الكبرى، في حين تستخدم هذه الجماعات فيسبوك في تجنيد أتباع جدد ونشر الأفكار والمعتقدات؛ لأنه أكثر الشبكات الاجتماعية انتشارا، أما موقع يوتيوب فهو ساحة افتراضية للتدريب؛ فالوظيفة الأساسية له استضافة الفيديوهات التي يقوم المشتركون بتحميلها.

ووفق صحف محلية مصرية، فقد عدَّد التقرير خصائصَ الإرهاب الإلكتروني، في أنه لا يترك أي دليل مادي بعد ارتكاب جرائمه، وهذا ما يصعب عملية التعقب واكتشاف الجريمة، وسهولة إتلاف الأدلة، كما أن مستخدمي هذا النوع من الإرهاب يمتازون بخبرات في استخدام التقنيات الحديثة، بالإضافة إلى أنه يحدث في بيئة هادئة لا تحتاج إلى القوة والعنف واستعمال الأسلحة.

وأشار التقرير إلى أن الجماعات الإرهابية، تستخدم المواقع الاجتماعية لتسهيل التحويلات المالية في ما بينها، إلى جانب الحصول على التبرعات، علاوة على تضخيم جرائمها من خلال نشر التحقيقات الإعلامية عن مقاتليها وتصويرهم كـ"جبابرة عتاة يثيرون الرعب"، مما يفقد المواطنين الثقة في حكوماتهم وقدرتها على حمايتهم.

وحدَّد التقرير ثلاث فئات تستهدفها الجماعات الإرهابية.

أولها:

المتعاطفون مع الفكر الإرهابي وهؤلاء غالبيتهم من الشباب.

ثانيها:

الرأي العام لأجل تأكيد نفوذ هذه التنظيمات في المجتمع، إما بغرض الحشد والتأييد أو التخويف من مواجهتها.

آخرها:

الخصوم من أجهزة الدولة ومؤسساتها، بهدف إضعاف موقفهم، والتأثير على هيبتهم، وإظهارهم بمظهر العاجز في مقابل قوتها.

ويشير مراقبون إلى أن داعش "يتألق" في البشاعة على الإنترنت لإعطاء الشعور بأنه مسيطر.

وأرجع المرصد في تقريره الأسباب التي تقف وراء استقطاب واجتذاب التنظيمات الإرهابية للشباب إلكترونيا، إلى الجهل والفقر والبطالة والتي تدفعهم إلى الالتحاق بتلك الجماعات، خاصة بعدما تستخدم المال لتغري به الشباب الحالم بمستقبل أفضل.

وأوضح التقرير أن تجنيد التنظيمات الإرهابية للشباب عبر الإنترنت يمر بثلاث مراحل تتعلق الأولى بـــ:

مرحلة التأثير الوجداني:

من خلال إثارة العاطفة والغيرة الدينية بحجة الدفاع عن القيم المقدسة، ويتم استخدام نصوص دينية عبر شبكات التواصل الاجتماعى، حيث أن 80% من مقاتلى التنظيم جندوا عبر الشبكات الاجتماعية.

المرحلة الثانية:

فتتعلق بدور الشبكات الاجتماعية في نقل المعلومات والبيانات، التي تعبر فقط عن وجهة نظر الجماعات الجهادية.

المرحلة الثالثة:

والتي هي أخطر المراحل، وتتعلق بالانتقال من مرحلة التأثير في الأفكار إلى المشاركة الفعلية في التغيير بالقوة والعنف وهو ما يظهر في التغيير السلوكي.

وأفرد التقرير صفحات محوره الأخير لعرض استراتيجيات القضاء على هذه الظاهرة، حيث طالب الحكومات بسن قوانين فعَّالة للتعامل مع جرائم الإرهاب الإلكتروني.

وحثَّ المرصد على إنشاء هيئة وطنية تهتم بمكافحة الإرهاب والجرائم المرتبطة بشبكة الإنترنت ووسائل التواصل الاجتماعي، تعطي صلاحيات واسعة لملاحقة هذه المواقع والمرتبطين بها، وتدشين المواقع التي تنشر الفكر الإيجابي.

كما طالب التقرير بحصر جميع ما يُثار من شبهات على شبكة الإنترنت والرد عليها من قبل الجهات المختصة ونشرها بنفس الطريقة من خلال المواقع الإسلامية، وضرورة التوسع في تنظيم المحاضرات والندوات واللقاءات التي تجمع بين العلماء والدعاة والشباب في حوار مفتوح للإجابة عن جميع الاستفسارات.

وحث التقرير مراكز البحوث على إجراء دراسات علمية ميدانية بدءا من البيئات الاجتماعية التي أفرزت العناصر الإرهابية وتحليل آرائهم للوقوف على جوانب الخلل[1].

إن المواقع الالكترونية لتلك المنظمات لاتخاطب أعوانها ومموليها فحسب بل توجه رسائلها أيضا للاعلام والجمهور وتقوم بترويعا وارهابها.. وبنفس الوقت يدعي الإرهابيون أنهم أصحاب قضايا نبيلة وهذا ما نجده في استخدام مواقع التواصل الاجتماعي وهو يجذب الملايين من الناس.. ومن هنا ينطلق الإرهاب واستطاع جذب شرائح المجتمع التي لم تحقق طموحاتهم الخاصة في الدين والسياسة والاقتصاد والعلم. وتضيف.. دائما يركزون على حاجات شخصية دقيقة..!! وأنهم (الجماعات الارهابية) يشكلون الخلاص الوحيد لمن يرى نفسه حائراً ضائعاً في متاهات حياته الخاصة. فشبكة مواقع التواصل سيف ذو حدين.. ترعب فيه من تريد ان ترعبهم وتكسب تأييد بعضهم[2].

وعن تاريخ الجماعات المتطرفة عبر الإنترنت، والتي سجلت عام 1995 كأول تجربة تبادل معلوماتي بين الجماعات المتطرفة عبر خدمة البريد الإلكتروني، يتبين أنه بعد انتشار خدمة الإنترنت وثورة نقل المعلومات والمواقع دخلت هذه الجماعات إلى عالم الإنترنت بقوة.

إلا أن التحريض الإلكتروني والنشر المسيء من الجماعات المتطرفة، خفّت وطأته في الآونة الأخيرة مقارنة بالأشهر السابقة، حيث أن هذا التراجع يعود إلى الهجمة الفكرية التوعوية القوية في مواجهة التطرف والإرهاب بجميع أشكاله، وتعالى النداءات الواضحة والصريحة للتعامل مع هذه المواقع، فقد تحركت شبكة "تويتر"وبقية شبكات التواصل الاجتماعي في شكل ملحوظ بإغلاق آلاف الحسابات المسيئة التي تدعو إلى العنف، أوالانتماء إلى جماعات إرهابية، أو الاعتداء على الآخرين لفظياً أو جسدياً أو معنوياً.

وكذلك إطلاق مواقع ومنتديات وشبكات، والتسلل إلى مواقع إسلامية حوارية كثيرة، وأفراداً لنشر أفكارهم وأدبياتهم.

1-http://www.alarab.co.uk/?id=58218.2016/7/1 ت/ د الجمعة

2- جوان فؤاد معصوم: بحث الارهاب الالكترونى، ورشة عمل بعنوان (مكافحة الارهاب ضرورة وطنية) ولفترة يومين 15 – 16 تشرين 2016 العراق.

هذا بالإضافة إلى ضرورة الحد من ظاهرة الإرهاب الإلكتروني في عصر المعلوماتية، وخصوصاً بعدما أصبحت ظاهرة عالمية تتطلب إيجاد حلول فعالة واتخاذ تدابير وقائية لوقف الزحف الخطر، الذي بات يهدد اقتصادات وأمن واستقرار الدول بعد تطورها من إطارها الكلاسيكي المعروف إلى التقنية العلمية الحديثة[1].

والجدير بالذكر أنه مادام هناك جريمة فلابد من وجود وسائل لإرتكابها بغض النظر عن نوع هذه الجريمة أو البيئة الحاضنة لها.

1- https://units.imamu.edu.sa/deanships/dialogue_civilizations/news/Pages/erhab-5.aspx
مصدر ملتقى الارهاب الالكترونى بتاريخ الاثلاثاء 2016/6/28

ثامناً: وسائل الإرهاب الإلكتروني.

أ- البريد الإلكترونى.

وعلى الرغم من أن البريد الإلكتروني (E.Mail) أصبح أكثر الوسائل استخدامًا في مختلف القطاعات، وخاصة قطاع الأعمال لكونه أكثر سهولة وأمنا وسرعة لإيصال الرسائل إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، من خلال استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرًا من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها.

وكذلك يقوم الإرهابيون باستغلال البريد الإلكتروني في نشر أفكارهم والترويج لها والسعي لزيادة الأتباع والمتعاطفين معهم عبر المراسلات الإلكترونية.

ومما يقوم به الإرهابيون أيضًا اختراق البريد الإلكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية.

ب- إنشاء مواقع على الإنترنت

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة نشر الفيروسات وغير ذلك[1]. فإذا كان الحصول على وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعبا، فإن إنشاء مواقع على الإنترنت، واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين غدا سهلًا ممكنًا، بل تجد لبعض المنظمات الإرهابية آلاف المواقع، حتى يضمنوا انتشارًا أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها[2].

جـ- غرف الدردشة.

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإرهاب والإجرام، وتبادل الآراء والأفكار والمعلومات صعبا في الواقع فإن الإنترنت تسهل هذه العملية كثيرًا، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد، ويتبادلوا الحديث والاستماع لبعضهم عبر الإنترنت، بل يمكن أن يجمعوا لهم أتباعًا وأنصارًا عبر إشاعة أفكارهم ومبادئهم من خلال مواقع الإنترنت، ومنتديات الحوار، وما يسمى بغرف الدردشةحيثتستخدم هذه الغرف في المواقع المتطرفة لأغراض تبادل المعلومات وتخطيط الهجمات والدعاية والانتشار ولجمع الأموال ولتجنيد الأتباع[3].

ويستوقفنا هنا تساؤل هام وهو **هل للتنظيمات الإرهابية سمات خاصة بها أثناء تعاملها مع شبكات الإنترنت؟**

1- يحي على دماس: دور تقنيات التواصل الاجتماعى فى التوعية بالعمليات الارهابية (جامعة نايف العربية للعلوم الأمنية،2013) ص31

2- فايز الشهرى: التطرف الإلكترونى رؤية تحليلية لاستخدامات شبكة الانترنت فى تجنيد الأتباع، مؤتمر استخدام التقنية فى الترويج للفكر الإرهابى، 2016.

3- فايز الشهرى: التطرف الإلكترونى رؤية تحليلية لاستخدامات شبكة الانترنت فى تجنيد الأتباع، مرجع سابق

تاسعاً: أبعاد وسمات أعضاء التنظيمات الإرهابية على الإنترنت:

1- الطابع التديني: تنطلق التنظيمات الإرهابية في البلدان العربية من منطلقات تدينيه، وترفع شعارات دينية، وتزعم أنها تعمل تحت مظلة دينية.

2- تدعى جميع التنظيمات الإرهابية في البلدان العربية أنها تخدم قضية وأنها تعمل في خدمة المصلحة العامة (الدينية والاجتماعية والوطنية)[1].

3- تحاول التنظيمات الإرهابية العربية استغلال ارتباك الكثير من الأنظمة العربية وتعثر خطواتها في إنجاز مهامها الوطنية والاجتماعية والثقافية لصالحها، وتسعى لاستغلال هذا الارتباك (وربما الفشل أحيانا)، والشعور بالإحباط الناجم عنه لصالحها، وتظهر بمظهر القوة التي تتبنى نضال الشعوب لإنجاز المهام الوطنية والاقتصادية والثقافية والدينية.

4- من المؤكد أن التنظيمات الإرهابية في المجتمعات العربية لم توجد في فراغ، وإنما ظهرت في سياق ظروف سياسية واجتماعية واقتصادية ودينية معينة، أنتجتها وربما ما زالت تعيد إنتاجها.

5- اعتماد التنظيمات الإرهابية في المجتمعات العربية أساساً على فئة الشباب المحبط بسبب معطيات الواقع العربي ومفرداته.

6- تتميز التنظيمات الإرهابية في المجتمعات الدينية بطابعها غير القطري، وبأنها عابرة للحدود القطرية، وذلك نتيجة للقضية العامة، التي تزعم أنها تعمل من أجلها.

1- http://www.assakina.com/book/45994.html
الإرهاب والجريمة الالكترونية بالمجتمع السعودي 1/7/2016ت/د الجمعة.

7- تحرص التنظيمات الإرهابية العربية على تحقيق التواصل الدائم مع الجماهير الواسعة من خلال استخدامها لوسائل الإعلام العامة، والإلكترونية (الإنترنت)، وإقامة صلات خاصة مع بعض الوسائل الإعلامية العربية (وخاصة الفضائيات التلفزيونية الواسعة الانتشار) واعتمادها على بعض الأوساط المتدينة المتعاطفة معها[1].

ولكن ثمة تساؤل يفرض نفسه: **هل دعم وتمويل التنظيمات الإرهابية يكون فقط عن طريق الأموال؟** الإجابة بالطبع لا فهناك سبل أخرى للدعم أهمها رأس المال الإجتماعى.

1- يوسف بن أحمد الرميح: الارهاب والجريمة الالكترونية بالمجتمع، مرجع سابق ص 224.

عاشراً: دور رأس المال الإجتماعي فى دعم الإرهاب الإلكترونى:

رصدت الدراسات الغربية تصاعد أعداد المقاتلين المنضمين للجماعات الإرهابية وتنوع الخلفيات الاجتماعية والثقافية والدينية بالإضافة إلى اختلاف جنسياتهم، مما دفع الباحثين الغربيين إلى محاولة معرفة التغيرات التي طرأت على عناصر قوة الجماعات الإرهابية وقدرتها على استقطاب متعاطفين ومتطوعين من خلفيات متنوعة.

وفي هذا الإطار توصل(فيكتور أسال) في دراسة له في فبراير 2015 بعنوان "**بناء الإرهاب من الروابط الاجتماعية: الجانب المظلم لرأس المال الاجتماعي**" أن هناك تحول واضح في عوامل قوة الجماعات الإرهابية فلم تعد تستند على الأيديولوجيات الفكرية أو الدعم المالي فقط بل ارتكزت على ما **يعرف برأس مال الاجتماعي، وهو ما يتركز في العلاقات العائلية** سواء كانت **قرابة أو نسب أو مصاهرة** وهو ما يتضح في علاقات الأخوة التي تربط بين (أيمن الظواهري ومحمد الظواهري)، وكذلك (سعد بن لادن الإبن الأكبر لأسامة بن لادن والمنضم أيضا لتنظيم القاعدة)، والمصاهرة عن طريق (زواج سليمان بن غيث أحد أعضاء القاعدة لإحدى بنات بن لادن).

ولا يقتصر الأمر علي العلاقات العائلية فقط بل كانت **لعلاقات الصداقة** دور كبير في دعم أواصر الجماعات الإرهابية، وهو ما ظهر في اعتماد داعش في استقطابها للشباب على أصدقائهم على الرغم من عدم اقتناعهم بمبادئ التنظيم، وأخيرا استناد الجماعات الإرهابية على **قاعدة شعبية في المناطق التي يسيطر عليها** مكنته من الحشد وجذب المتطوعين وهو ما اتضح في استطلاعات الرأي في مناطق تمركز تنظيم القاعدة وطالبان أثبتت أن (47%) يروا أن أنشطة القاعدة تهدف إلى تحقيق العدالة ونصرة المسلمين في العالم وهو ما يمثل تحول خطير في الظاهرة الإرهابية.

وفي ذات السياق أكد (لورانس روبين) في دراسة له منشورة في يوليو 2015 بعنوان "**لماذا لن تصبح داعش دولة طبيعية"؟**، لأن قوة داعش ترجع إلى السمات الشخصية للقيادة فأبو بكر البغدادي لدية قدرة على إلقاء الخطب مستخدماً في ذلك اللغة العربية الفصحى بالإضافة إلى أصله القرشي وفق إدعاء تنظيم داعش مما

أكسبه مكانة بين أعضاء التنظيم، يضاف إلى ذلك تأثير المكاسب العسكرية التي حققها وقدرته على التحكم في أعضاء التنظيم والسيطرة على المناطق التي تقع تحت قيادته، مما مكنه من جذب أعداد كبيرة من المقاتلين الأجانب وظهور المزيد من التنظيمات التي أعلنت ولائها لداعش، فضلاً عن الاهتمام الإعلامي بالتنظيم والسعي نحو تضخيم أهميته[1].

فالانضمام إلى هذه التنظيمات لا يكون وليد اللحظة، فمرتكب العنف والارهاب لابد أن يكون لديه فكر معين لم يستطع اقناع الناس به فلجأ إلى إجبارهم على فعل مايريد بالعنف، كما أننا لا نستطيع القول بأن كل هؤلاء الإرهابيون مأجورون، فبعضهم مأجور ولكن السواد الأعظم منهم مقتنعون بما يفعلون هذا الاقتناع يأتى نتيجة تعامل فكرى معين من قبل هذه التنظيمات مع الشباب لذلك تكوين العقل المتطرف **يمر بعدة مراحل تتمثل فى المراحل الأتية**[2].

1- http://www.rcssmideast.org/Article/ رؤى المراكز البحثية الغربية للإرهاب في الشرق الأوسط 25/01/2016

2- الباحثة.

حادى عشر: مراحل تكوين العناصر المتطرفة على الإنترنت:

المراحل التي يتدرج المتطرفون من خلالها لإيصال أفكارهم واستقطاب المزيد من الأتباع عن طريق:

المرحلة الأولى:

ضخ الفكر المتطرف من خلال البحث في الكتب والفتاوى وإظهار التفسيرات الأكثر تشددا للنصوص وإنزالها على وقائع العصر ومن ثم إصدار الأحكام. وفي هذه المرحلة يكون الشاب في مرحلة التأمل والاختيار.

المرحلة الثانية:

المساعدة في الاختيار وهي مرحلة يتم من خلالها استخدام المؤثرات لدفع الشخص الحائر لتكوين موقف.

المرحلة الثالثة:

التهنئة على معرفة "الحق" وتعزيز الأفكار الجديدة حينما تلوح بوادر اقتناعه ببعض الأفكار.

المرحلة الرابعة:

الانضمام الفعلي للتنظيم تحت شعار الهداية والالتزام وطلب الجنة.

المرحلة الخامسة:

الانخراط في الأدوار العملياتية وهي الغاية الأساسية من كل هذه الجهود, فالتطرف لا ملة له ولاجنس[1].

لذلك فإن هذه التنظيمات لا تعمل بشكل عشوائى ولكنها تعمل وفقا لمنهج محدد يتمثل فى:

1- فايز الشهرى: التطرف الالكترونى سمة المجتمعات عصر العولمة، جريدة الرياض، العدد14411، 8 ديسمبر 2007.

ثانى عشر: منهج التنظيمات الإرهابية فى السيطرة على عقول الشباب.

1- بناء منظومة من القناعات الفكرية حول المجتمع والسياسة والحكم والحياة.

2- التشكيك ونقد القناعات المستقرة عند الناس خاصة في الجانب السياسي.

3- التباهي بمجتمع (الصفوة الجديد) الذي ينتمون إليه مع ذم المجتمع الغارق في شهواته وجهله وتنفير الشباب من هذه المجتمعات "الغارقة في ملذاتها".

4- تشويه سيرة العلماء والدعاة من خارج الفكر وتتبع عثراتهم واتهامهم بمداهنة السلطات وبيع الذمة.

5- تمجيد أسماء وسيرة شخصيات معاصرة وتاريخية وانتقاء ما يتناسب من مواقفها وآرائها لدعم وتعزيز الخط الفكري والعسكري لهذه التنظيمات.

6- نسف الأفكار الوسطية وبناء أساس فقهي جديد يعتمد على الأفكار المتشددة كبديل وترويجها بين الشباب باستثمار حماسهم وقلة معرفتهم الشرعية.

7- هدم الرموز الفكرية التي اعتاد الناس التوجه لهم كمراجع في مختلف القضايا وإعلاء أسماء رموز الفكر المتطرف كبديل نزيه في عالم يسوده "الظلم" "والخيانة".

8- الاغتيال المعنوي للرموز السياسية واتهامهم بالعمالة والمداهنة والطغيان وأن هؤلاء ماهم إلا "طواغيت" مسلطين على "شباب الجهاد".

9- الاندساس بين المحافظين ورفع صوت الاحتجاج على بعض المخالفات وإثارة العامة[1].

لذلك فالمتتبع للخطاب الفكرى الاسلامى على شبكة الانترنت يكتشف أن هناك ثلاث مدارس فكرية مهيمنة على الخطاب الفكرى الإسلام يعلى الشبكة العنكبوتية على النحو الآتي:

1- فايز الشهرى: الوجه التقنى للعنف: الانترنت نموذجا، جريدة الرياض، العدد13327، 19 ديسمبر 2004.

ثالث عشر: مدارس الخطاب الفكري الإسلامي على الشبكة العنكبوتية.

1- مدرسة الخطاب التقليدي.

وتنتهج مبادئ فكرية عادة ماتكون تابعة لمؤسسات رسمية أوشبه رسمية، أو لشخصيات ورموز فكرية إسلامية ذات خط فكري محافظ. ويمكن ملاحظة حضورها من خلال مواقع ومنتديات إلكترونية تتسم بوجود أطروحات فكرية يغلب عليها الهدوء والتركيز على مسائل التأصيل العقائدي والفتاوى، ولا تتطرق بشكل واضح إلى بعض الإشكاليات العصرية خاصة تلك التي تتعلق بالقضايا السياسية الشائكة أو مايختص بالجدل الدائر مع الآخرين من غير المسلمين، مع وضوح لغة اقصائية قوية مع المخالفين خاصة من تسميهم هذه المدرسة بالحزبيين من الجماعات الإسلامية.

2- مدرسة الخطاب الحركي.

هى نتاج بعض المجموعات الفكرية وعدد من المفكرين الإسلاميين الناشطين الذين اتجهوا إلى الإنترنت كوسيلة إعلام متاحة، ووجدوا فيها مجالاً للحركة ونشر أفكارهم التي تتميز عادة ببعض الجرأة، والكثير من مؤشرات الانخراط في القضايا السياسية وفق منهج توافقى فيه قدر من التصالح، وغير متضح الملامح مع المخالفين من أصحاب المدارس الفكرية الأخري[1]. ويلاحظ في حوار اتمنتسبي هذه المدرسة الاكتفاء بالتلميح – مدحاً أو قدحاً – عند ذكر الأنظمة والرموز السياسية القائمة، مع حرصه على الحفاظ على كثير من الخطوط الفكرية المشتركة مع علماء المدرسة التقليدية.

---

1 - فايز الشهرى: ثقافة التطرف والعنف على شبكة الانترنت الاتجاهات والملامح، مركز الدراسات والبحوث، 2012.

3- مدرسة الخطاب المتشدد.

وينطبق وصف الخطاب المتشدّد - هنا - على اطروحات مجموعات انتهجت المصادمة الفكرية والعسكرية مع مجتمعاتها، وتتضح خصائص منهج المتشددين هنا من خلال مواقعهم ومنتدياتهم ويتسمون بخطابهم التصادمي الرافض للواقع بلهجة حماسية تعتمد على التأثير العاطفي وبعث الحماس والغيرة لدى الشباب وقد قدم الإنترنت لهذه الجماعات خدمة كبرى كونها المنفذ الوحيد للتواصل والاتصالات مع المتعاطفين والأنصار وغيرهم. وتتميز لغة الخطاب في منتديات ومواقع هذه الجماعات بالحدة والانفعال مع الخصوم وتهيمن على موضوعاتهم لغة انفعالية عاطفية لاتقبل المخالف ولاتحاوره وفق منهج يتسم بالتحدي والإثارة، وفي معظم الطرح الفكري لبعض هذه الجماعات يمكن ملاحظة الكثير من مؤشرات السذاجة السياسية وعدم الكفاءة الفكرية في قراءة حقائق الواقع السياسي والعسكري[1].

وبعد ما تم استعراضه سابقا هناك تساؤل يطرح نفسه بشدة **هل مواقع التواصل الإجتماعى أداة لإرتكاب الإرهاب أم أنها وسيلة لمكافحته أم الإثنين معا؟**

فى حقيقة الأمر أن مواقع التواصل الإجتماعى هى الإثنين معا فى أداه لإرتكاب الإرهاب وكذلك يمكن أستغلالها كوسيلة لمكافحته **وفيما يلى استعراض لكيفية استغلالها فى الحالتان سالفتا الذكر.**

1- فايز الشهرى: التطرف الإلكترونى رؤية تحليلية لاستخدام شبكة الإنترنت فى تجنيد الاتباع، مؤتمر تقنية المعلومات والأمن الوطنى، الرياض، فى الفترة من 1-2007/12/4، ص19.

رابع عشر: توظيف مواقع التواصل الاجتماعى فى خدمة الارهاب ومكافحته.

قبل البدء فى تحديد دور مواقع التواصل الاجتماعى فى خدمة الارهاب **لابد أولا من إلقاء الضوء على عدة نقاط هى:**

تعريف الشبكات الاجتماعية.

1- هى مصطلح يطلق علي مجموعة من المواقع علي شبكة الإنترنت، تتيح التواصل بين الأفراد فى بيئة مجتمع افتراضى يجمعهم حسب مجموعات اهتمام أو شبكات انتماء (بلد - جامعة – مدرسة - شركة،.....) كل هذا يتم عن طريق خدمات التواصل المباشر مثل ارسال الرسائل أو الاطلاع على الملفات الشخصية للأخرين ومعرفة أخبارهم ومعلوماتهم التى يتيحونها للعرض، ومن أشهر الشبكات الاجتماعية هى: موقع فيس بوك وتويتر، وماى سبيس، وأوركت، وهاى فايف.

كما يمكن تعريفها على أنها:

2- خدمة إلكترونية تسمح للمستخدمين بإنشاء وتنظيم ملفات شخصية لهم، كما تسمح لهم بالتواصل مع الأخرين[1].

1- لمياء محسن محمد حسن: شبكات التواصل الاجتماعية العربية والعالمية، مجلة الاذاعة والتليفزيون، العدد الأول- يناير – مارس 2015، ص378 .

أهم ايجابيات شبكات التواصل الاجتماعى:

علي سبيل المثال وليس الحصر أنها تتيح فرصة للجمهور بالانفتاح على بيئات جديدة، والتعرف على أصدقاء جدد، كما أنها مصدر للتواصل بين الناس مهما تباعدت المسافات، ووسيلة للتعبير عن الرأى بحرية ودون قيود، ومصدر هام للمعلومات والأخبار، وأداة لتشيكل الرأى والاتجاهات سواء السياسية أو الاجتماعية، كما أنها وسيلة لترويج الأفكار، وحتى المنتجات والخدمات.

ولكن التكنولوجيا مثل مالها من مميزات وايجابيات تعود بالنفع على المجتمع فلها سلبيات كبيرة يعانى منها المجتمعات على سبيل المثال وليس الحصر.

أهم سلبيات شبكات التواصل الاجتماعى:

أنها تصرف مستخدميها عن الواقع الاجتماعى المحيط والإنغماس فى عالم افتراضى مما يسبب العزلة الإجتماعية للأفراد، وتفكك الأسرة، والإندماج والإنخراط وسط خضم من الأفكار غير المنقحة سواء كانت سياسية أو دينية، كما أنه يجعل المستخدمين عرضة للشائعات والأخبار المغلوطة، وكذلك انحراف الشباب لما تحتويه من مواقع إباحية تحرض على الرذيلة، وأخير أصبحت وسيلة لإستقطاب الشباب للتنظيمات الإرهابية عن طريق تجنيدهم وتبادل المعلومات معهم وتسميم أفكارهم من خلال زعزعة الثوابت والحقائق لديهم مما يهدد أمن المجتمع[1].

1- الباحثة.

"ولشبكات المعلومات والانترنت ايجابيات بالنسبة إلى التنظيمات الإرهابية خلقت منها أداة لإرتكاب الإرهاب أبرزها":

1- المرونة.

2- قلة المخاطرة.

3- قلة التكلفة المادية.

إذ أن جهاز حاسوب لا يزيد ثمنه على 500 دولار يستطيع أن يشن هجمات من خلاله تكلف الطرف الاخر ملايين الدولارات. وأكد أن "حواسيب وزارة الدفاع الاميركية تلقت 32 ألف هجمة في عام واحد أي بمعدل 60 الى 80 هجمة يوميا"[1].

وسهولة الحصول عليها ما سيمكن الإرهابيين، والمجرمين كغيرهم من أفراد المجتمع الإنساني من توظيف معطيات التقنية الحديثة، في خدمة أغراضهم أيّا كانت هذه الأغراض[2].

4- يمكن إخضاعه للسيطرة أو القيود.

5- وغير مراقب.

6- ويتيح حرية الوصول لكل من يريده.

1- جريدة الرأى، العدد13585، السبت 10 سبتمبر 2016.

2- فايز الشهري: التطرف الالكترونى على شبكة الانترنت رؤية تحليلية، مؤتمر تقنية المعلومات والأمن الوطنى، 12-14 /2008/11.

7- وتعتبر الشبكات الإرهابية الحديثة المألوفة، المكونة من خلايا غير محكمة الترابط وشُعب وجماعات فرعية، الإنترنت مثالي وأساسي للاتصال بين أعضاء المجموعة الواحدة وبين المجموعات المختلفة[1].

وما يزيد من ايجابيات الشبكة بالنسبة للتنظثيمات الإرهابية عدم استغلال الحكومات والجهات المعتدلة لهذه المواقع من أجل الحوار، ونشر ثقافة التسامح، والوسطية، والاعتدال في المجتمع، والتواصل مع الفئات المختلفة للتصدي للإرهاب، وكشف أساليبه، ومعتقداته، وفي صياغة رأي عام مضاد للإرهاب؛ مما مهد الطريق لهذه الجماعات لاستغلال هذا الفراغ وتسخير مواقع الانترنت لنشر أفكارهم المنحرفة، وتنفيذ عملياتهم الإرهابية[2].

ولكن مثل ما كانت مواقع التواصل أداة لإرتكاب جرائم الارهاب، يمكن أيضا أن تكون وسيلة لمكافحته.

1- 3 ايلول / سبتمبر 32008

http://iipdigital.usembassy.gov/st/arabic/publication/2008

2- فايز الشهرانى: الأنترنت سلاح الإرهاب الجديد، جريدة الرياض- العدد 16985،25 ديسمبر 2014م.

توظيف مواقع التواصل فى محاربة الارهاب الالكترونى.

1- فحص محتوى الشبكات بشكل دورى وإزالة كل مايحرض على الارهاب مثل قيام وحدة مكافحة الإرهاب على الإنترنت في بريطانيا بإزالة 65 ألف محتوى من الإنترنت كان يدعو إلى الإرهاب، منها 46 ألف منذ ديسمبر الماضي، حيث أن 70 بالمائة من هذه الموضوعات كانت تدور حول الأحداث في سوريا والعراق.

2- إغلاق بعض الصفحات التى تحرض على العنف، مثل قيام موقع فيسبوك بإغلاق الصفحة الخاصة بمايكل أديبويل الذي أقدم على قتل جندي بريطاني، بعد أن نشر على صفحته في الموقع رغبته في "قتل جندي بطريقة وحشية" قبل 5 أشهر من إقدامه على ذلك بالفعل في حادثة "وولويتش" الشهيرة، دون أن يبلغ الموقع السلطات بهذه الخطوة[1].

3- انشاء مواقع وصفحات من شأنها نشر الأفكار المضادة للإرهاب والتوعية بخطورته على أمن وسلامة المجتمعات.

4- استحداث قوانين جديدة لمواقع وشبكات الانترنت بحيث يمكنها منع المواقع والصفحات ذات المحتوى العنيف والإرهابى قبل بثها على الناس انطلاقا من مبدأ الوقاية خيرا من العلاج[2].

1- الارهب الالكترونى والشبكة العنكبوتية بتاريخ 2014/12/24.
2- الباحثة.

خامس عشر: العلاقة بين الإعلام والإرهاب.

ومن الزاوية الإعلامية المجردة نجد أن العمليات الإرهابيّة - حتى قبل الانترنت وثورة الاتصال- عادة ما تحظى بتغطيات إعلاميّة مكثفة، حيث تجد فيها وسائل الإعلام مادة صحفية مثيرة فتتناولها بشكل مركز وفق منطق (الحدث الإرهابي، حدث إعلامي). ولعل هذا ما دعا بعض الخبراء إلى التحذير من أن وسائل الإعلام قد تنحرف - تحت ضغط المنافسة - عن دورها في البناء الاجتماعي، إلى الترويج للإرهابيين الذين يستغلون بمهارة مسألة حرص الإعلاميين على السبق الصحفي، لتمرير أيدلوجية معينة أملا في كسب تعاطف الرأي العام مع قضاياهم. وربما يكون في هذا الكلام شيء من الصحة مع أن الإرهاب في الأصل يعتمد العنف لتحقيق أهدافه إلا أن نشر القضية التي يؤمن بها الإرهابيون ويناضلون من أجلها لا يتأتى إلا بتسليط الضوء الإعلامي المكثّف عليها. ولأن وسائل الإعلام التقليدية تعمل تحت سيطرة أنظمة ومؤسسات وتعمل وفق حسابات ومصالح، فقد برزت الانترنت كوسيلة حرّة وجماهيرية مغرية للجماعات الإرهابية التي بادرت إلى استغلالها كأفضل قناة مرنة للإعلام والاتصال بالجماهير.

ووفقا لذلك لم تعد صورة الإرهابي المعاصر تشبه تلك الصورة النمطية للإرهابى التقليدي، الذي يقاوم، ويدمّر، ويخطف الطائرات، فقد أصبح عنصر الجماعة الإرهابية اليوم أكثر ارتباطا بالتقدم التقني، ويوصف عادة بالذكاء الاستثنائي، بل ويبدو في الخيال الشعبي بهيئة عصرية جذّابة، فهو يرتدي البدل والملابس الأنيقة، ويستخدم الهواتف النقالة ويستخدم أجهزة الحاسب المحمولة ليدير عملياته، ويجري اتصالاته بالأعوان، من وإلى أي مكان في العالم[1]. والذى يرسم هذه الصورة سواء التقليدية أو المعاصرة وسائل الإعلام نفسها، وهناك العديد من المعالجات التى تستخدمها وسائل الاعلام لتغطية أحداث الإرهاب[2].

1- فايز الشهرى: الوجه التقنى للعنف، الانترنت نموذجا، جريدة الرياض – العدد13327،2004.
2- الباحثة.

أولاً: تحديد نوع المعالجه الاعلاميه لقضايا الارهاب:

وبخصوص تحديد نوع المعالجة الإعلامية لقضايا الإرهاب، توجد نظريتان رئيسيتان تطرحان مدى تأثير التغطية الإعلامية للإرهاب على الرأي العام، **وهما كالآتى:**

أ- نظرية العلاقة السببية بين الخطاب الإعلامي والإرهاب:

ووفقاً لهذه النظرية فإن التغطية الإعلامية للإرهاب تؤدي إلى انتشار ظاهرة الإرهاب، حيث تتكاثر العمليات الإرهابية كنتيجة طبيعية للتغطية الإعلامية.

وحسب هذه النظرية هناك ثلاثة أنواع للتأثيرات الإعلامية:

أولها: الوعي والتبني.

ثانيها: انتشار العدوى.

ثالثها: الوساطة.

الوعي والتبني:

يشيران إلى أن التغطية الإعلامية لحوادث الإرهاب ترفع مستوى وعي الجماهير عامة والجماعات الأكثر ميلا خاصة.

إنتشار العدوى:

يعني أن التغطية الإعلامية تفرز العديد من العمليات الإٍرهابية.

الوساطة:

تعني إمكانية وجود تدخل فعلي من جانب الصحافيين، للوساطة بين الإرهابيين ورجال الشرطة أو المسؤولين بالدولة. وتدعو هذه النظرية الحكومات إلى المزيد من القيود على وسائل الإعلام، فهي تفترض أن وسائل الإعلام ترتبط عضويا بالإرهاب، فالإرهاب يعتمد على الإعلام لتحقيق المزيد من الفزع في أوساط الجماهير وللحصول على الشرعية لدى السلطة، في المقابل يعتمد الإعلام على التهويل في تغطيته للإرهاب بقصد تحقيق أكبر ربح ممكن من خلال زيادة المبيعات. فالعلاقة بين الطرفين تأخذ شكلاً دائرياً لا ينتهي، حيث يستفيد كل طرف منهما من الطرف الآخر.

والتصور العلمي فى هذا الشأن يرى أن وسائل الإعلام ضحية للإرهاب، فهي إما تتناول الحدث الإرهابي وتحقق أثراً نفسياً مروعاً، وإما تتجاهله بسبب قيود الحكومات فتفقد بذلك مصداقيتها.

ب- نظرية الخطاب الإعلامي والإرهاب والعلاقات المتباعدة:

يرى أصحاب هذه النظرية أنه لا يوجد دليل علمي على أن التغطية الإعلامية للإرهاب هي المسؤولة عن مضاعفة العمليات الإرهابية، فليس هناك أية علاقة قائمة بين المتغيرين، ولهذا يدعوا أصحاب هذه النظرية إلى عدم التدخل في أداء وسائل الإعلام عامة وفي علاقتها بالإرهاب خاصة، لأنه من غير المعقول حسب رأيهم أن تكون هناك علاقة بين الطرح الإعلامي لقضايا الإرهاب وزيادة معدّله. علاوة على هذا فهم يرون في أن حرمان الإرهابيين من الوصول إلى وسائل الإعلام يُساهم في زيادة معدّل الإرهاب، لأن الإرهابي يريد أن تصل رسالته إلى الطرف الثالث، وفي حالة عدم وصولها من خلال وسائل الإعلام، سيعتمد الإرهابيون على تكرار الأحداث باستخدام وسائل أكثر بشاعة في مختلف الأماكن وعبر فترات زمنية مختلفة، ليحققوا بذلك خسائر مادية وبشرية كبيرة، تُمكنهم من إيصال رسالتهم وتحقيق أهدافهم.

ومن الشروط والفرص التي تضمن للإرهابيين إشهاراً واسعاً، نجد على سبيل المثال:

اختيارهم المتعمد لأوقات محددة، وأماكن معينة لتنفيذ عملياتهم الإرهابية **فمثلا:**

لعبت الصحافة المكتوبة اليومية بإيطاليا دوراً مركزياً، حيث كان الإرهابيون الإيطاليون لليسار المتطرف غالبا ما يوجهون ضرباتهم أيام الأربعاء والسبت، وهي الأيام التي يكون فيها سحب الجرائد كبيراً.

فالإرهابيون حاليا يحددون القنوات الفضائية التي يتعاملون معها خاصة أثناء تنفيذهم لعمليات إرهابية، وضَمنت هذه الطريقة للعمل الإرهابي مزيداً من قوة التأثير في الجمهور من خلال وسائل الإعلام المنتقاه التي أصبحت تقدم المزيد من التنازلات للإرهابيين، مقابل انفرادها بتغطية عملياتهم ونشر وثائقهم وبياناتهم وتصريحاتهم.

فهناك بعض المتخصصين الإعلاميين يرون أن العلاقة بين الإعلام والإرهاب أصبحت في الوقت الحالي عبارة عن شراكة بين مؤسستين، إحداهما تقوم بصنع الحدث والأخرى تسوقه[1].

1- نصيره تامى: **"دور الاعلام الفضائى فى التصدى لظاهره الارهاب: الاعلام الفضائى العربى.. نموذجاً"** Htm144191http://temmaryoucef.ab.ma/

ثانياً: الأخطاء التي تقع فيها وسائل الإعلام أثناء تغطية الأعمال الإرهابية.

يمكن تحديد أبرز سمات المعالجة الإعلامية العربية للظاهرة الإرهابية وللعمليات الإرهابية **على النحو التالي:**

1- التركيز على الحدث أكثر من التركيز على الظاهرة. يعطي الإعلام العربي اهتماماً للعمليات الإرهابية أكثر من الاهتمام الذي يعطيه للإرهاب كظاهرة لها أسبابها وعوامله.

2- هيمنة الطابع الإخباري على التغطية الإعلامية العربية للعمليات الإرهابية، وتقديم تغطية متعجلة وسريعة، وربما أحياناً سطحية، تهتم أساساً بتقديم جواب عن سؤال: ماذا حدث؟! وتغيب في الغالب، التغطية الإعلامية ذات الطابع التفسيري والتحليلي، كما تغيب التغطية ذات الطابع الاستقصائي، الأمر الذي يؤدي إلى بقاء المعالجة الإعلامية على سطح الحدث والظاهرة.

3- تتوارى في الغالب، معالجة جذور الظاهرة الإرهابية وأسبابها العميقة السياسية والاجتماعية والاقتصادية والدينية، وهذا ما يجعل الظاهرة تبدو وكأنها مجردة ومطلقة، وتقع خارج حدود الزمان والمكان والمجتمع، وهذا ما يضعف قدرة التغطية على الإقناع، لأنه يفقدها طابعها الملموس .مع غياب الخبراء والمختصين في المجالات سالفة الذكر .

4- لا يتوفر لدى الكثير من وسائل الإعلام العربية كادر إعلامي مؤهل ومختص، قادر على تقديم معالجة إعلامية مناسبة لهذه الظاهرة المعقدة والمتشابكة والمتعددة الأبعاد خاصة بعد ظهور البعض من غير المحترفين على الساحة الإعلامية فى الأونة الأخيرة.

5- تتميز التغطية التي يقدمها الإعلام العربي للظاهرة الإرهابية بعدم الانتظام وعدم الاستمرارية، ولذلك تأتي هذه التغطية متقطعة، حيث تزداد كثافتها أثناء العمليات والمناسبات والمؤتمرات، ثم تضعف، وتتوارى، وربما تختفي نهائياً وهذا ما يؤثر سلبياً في قوة تأثيرها

6- تقع هذه التغطية في أحيان كثيرة في فخي التهوين أو التهويل بالظاهرة الإرهابية وهذا ما يؤثر سلبياً على مصداقية هذه التغطية وعلى مقدرتها على الوصول والتأثير .

7- تفتقر الممارسة الإعلامية العربية إلى وجود أي قدر من التعاون والتنسيق على المستوى العربي من أجل تقديم تغطية ذات طابع عربي عام ومشترك لهذه الظاهرة .

استناداً إلى ما تَقَدَّم يمكن تقسيم سمات التغطية الإعلامية العربية للظاهرة الإرهابية إلى نوعين أساسيين:

1- سمات ذاتية:

توجد أسبابها في الظروف الذاتية للمؤسسة الإعلامية، ويقع حلها بالتالي داخل هذه المؤسسة، بمعنى أن حلها إعلامي، يتعلق بالأداء الإعلامي وبالمهارات الإعلامية .

2- سمات موضوعية:

توجد أسبابها في الظروف الموضوعية السائدة في جوانب متعددة في حياة الدولة والمجتمع، ويقع حلهابالتالي، خارج إطار المؤسسات الإعلامية، بمعنى أن حلها ليس إعلامياً، بل هو سياسي واجتماعي واقتصادي وثقافي .

فوسائل الإعلام تقوم عن غير قصد بالترويج للخطاب الإرهابى على نحو يؤدى إلى تحفيز فئات اجتماعية مطحونة، أو جماعات عرقية وقومية ومذهبية مهمشة إلى سلوك سبيل الخيار الإرهابى العنيف للإعلان عن مطالبها الحقوقية. من ناحية أخرى قد تؤدى بعض التغطيات الإعلامية عن العمليات، وتضارب المعلومات والأخبار والقصص حولها إلى بث بعض من البلبلة والغموض، مما قد يؤدى إلى هروب بعض الفاعلين، أو عدم القدرة على تحديد الجهات القائمة بالعمل الإرهابى. ففى بعض الأحيانتؤدى بعض التغطيات الإعلامية محدودة المستوى والكفاءة المهنية إلى خلق تعاطف بعض الجمهور مع الإرهابى. ومن ناحية أخرى، قد يشكل الإعلام فى بعض الأحيان دور الوسيط بين القائم بالإرهاب، والمستهدف سياسياً بالعملية الإرهابية[1].

1- الاعلام والارهاب: استراتيجية المواجهة، شبكة الاخبار العربية، 10 سبتمبر 2016.

جـ- الدور المعرفى والتنويرى للإعلام فى مواجهة الإرهاب.

ولكننا لا نستطيع اتهام الإعلام بأنه اللاعب الرئيسى فى نشر الإرهاب والترويج له حتى فى ظل ما يرتكبه الاعلام من أخطاء سبق ذكرها،ولكن الإعلام أيضا سلاح مهم ضد الإرهاب يمكن استغلاله فى وأد فكرة الإرهاب من الأساس من خلال الدور التنويرى والمعرفى للإعلام والذى يتمثل فى معالجة موضوع تجديد الخطاب الديني باعتباره ضرورة حتمية في المواجهة الثقافية للإرهاب، وحتى يقوم الإعلام بدوره التنويري المفتقد، فلا بد من التركيز على أهمية تكوين "العقل النقدي" باعتبار ذلك البداية الضرورية لتجديد الفكر الديني. وهناك في مجال إبراز الدور المعرفي للإعلام في مواجهة الإرهاب موضوعات شتى لا يمكن الاستفاضة في تفاصيلها.

ولكن نستطيع أن نشير إلى أبرز معالمها. وأول هذه الموضوعات هو:

ضرورة إلقاء الضوء على تأويل الإرهابيين للنصوص الإسلامية وتقديم صورة نقديه لها نابعة من القرأن والسنة. وهذا موضوع بالغ الأهمية، لأن الجماعات الإرهابية استطاعت عن طريقه، باستخدام ما يطلق عليه "آلية القياس الخاطئ والتأويل المنحرف"، أن تبرر منطق تفكيرها المنحرف، وتضفي الشرعية على أساليبها الإجرامية التي تتمثل في ذبح الرهائن علناً أو إحراقهم أو إغراقهم ونشر ذلك على وسائل الإعلام المختلفة بالصوت والصورة، لبث الرعب في القلوب وإظهار أن قوتها التدميرية لا حدود لها.

ولذلك، فإن مقولات مثل: (جاهلية المجتمعات العربية والإسلامية)، أو (تكفير غير المسلمين باعتبارهم كفاراً يجوز قتالهم في الداخل أو في الخارج)، بل وقتل المسلمين الذين يتبعون "الطواغيت"، أو الحكام العرب والمسلمين الذين لا يطبقون شرع الله في نظرهم، كل هذه المقولات تحتاج إلى تفنيد بنشر التفسيرات الصحيحة من الكتاب والسنّة، حتى لا تنخدع الجماهير بالخطاب التحريضي لهذه الجماعات الإرهابية.

أما الموضوع الثاني المهم هو:

تشريح العقل الإرهابي – إن صح التعبير – من وجهة نظر العلم الاجتماعي بفروعه المتعددة، مثل علم الاجتماع وعلم النفس، لبيان كيف يتشكل هذا العقل، وما هي الآليات الأساسية التي تطبقها الجماعات الإرهابية في تشكيله، وكيف يمكن رسم سياسة متكاملة لتغيير اتجاهات أعضاء التنظيمات الإرهابية والمتعاطفين معها حتى تتبدل رؤيتهم للعالم التي تتسم بالانغلاق والتعصب ومعاداة غير المسلمين وتكفير المسلمين. ولا بد من رصد التفاعل والصراع بين الذات الإرهابية والمجتمعات العربية والإسلامية المعاصرة لبيان المجالات التي يشتد فيها الصراع، سواء بالنسبة إلى نسق التربية داخل الأسرة، أو نوع النظام التعليمي، أو الموقف من المرأة، أو رفض الفنون والآداب، أو اعتماد الماضي باعتباره المرجعية الأساسية التي يعتمد عليها لرسم قواعد السلوك في الحاضر أو في المستقبل، بغض النظر عن تغير الأزمان وعدم مطابقة التفسيرات التقليدية للأوضاع العالمية الراهنة.

وهناك في تجارب الدول العربية خلال مواجهتها موجات الإرهاب، خبرات تستحق الدراسة، خصوصاً في السبعينات في بلد مثل مصر نشطت فيه جماعتا "الجهاد" و"الجماعة الإسلامية" الإرهابيتان. واستطاعت الحكومة المصرية أن تقيد حركة هذه الجماعات وتعتقل الألوف من أعضائها ممن ارتكبوا أفعالاً إرهابية في السجون والمعتقلات، التي قام قادة هذه الجماعات فيها "النقد الذاتي".

ويبقى أمامنا توضيح الدور التنويري البالغ الأهمية الذي على الإعلام العربي القيام به، والذي يعاني في الواقع من إهمال شديد، لعدم الوعي الكافي بأهميته القصوى. هذا الدور التنويري يتلخص في عبارة واحدة هي "أهمية تأسيس العقل النقدي العربي" الذي يطرح كل ما في الطبيعة والمجتمع للتساؤل، بدلاً من سيادة "العقل الإتباعي" الذي يقوم على التسليم بما هو سائد من معتقدات وآراء وسياسات تجاوزها الزمن الذي نعيش فيه، ونعني عصر العولمة بكل الإنقلابات الكبرى التي أحدثها في حياة البشرية[1].

1- http://www.alhayat.com2016/9/1 مصدر تاريخ الدخول الخميس الموافق

لذلك وجب على الإعلام معرفة الجماهير وتنويرهم وزيادة وعيهم بأمور الدين القائمة على الكتاب والسنة ومن خلال المتخصصين فى هذا الشأن، وكذلك بيان كيفية تسلل الجماعات والتنظيمات الإرهابية إلى الجمهور وخاصة الشباب الذين يمثلون النواة الرئيسية لهذه التنظيمات ومراحل عمليات التجنيد والمنهج المتبع فى ذلك، وكيفية استدراج الشباب وزلزلة معتقداتهم الراسخة حول ثوابت الدين أو قيم وأخلاقيات المجتمع[1].

1- الباحثة.

سادس عشر: طرق مكافحة الإرهاب الإلكترونى:

هناك تنافس بين كل من رجال الشرطة والمجرمين فى استخدام الأساليب التكنولوجية التى تحقق أهدافهم، فقديما كان كل منهم يعمل إما على الأقدام أو امتطاء ظهور الخيل، ثم استعمل كلا الفريقين الدراجات ثم السيارات والطائرات وحاليا يستخدمون أجهزة الحاسب الآلى وشبكة المعلومات الدولية المعروفة بالإنترنت، وقديما استعان كل منهم بالبنادق والمدافع الرشاشة، كما يرتدى كلا الطرفين السترات الواقية من الرصاص، كما تم الاستعانة بالعربات المصفحة والقنابل المسيلة للدموع وأقنعة الغازات، كما يستخدم المجرمون الأشرطة اللاصقة، وأنه كلما استخدمت الشرطة أسلوباً تكنولوجياً، لجأ المجرمون لاستخدام أسلوب للوقاية منه، فحينما بدأت الشرطة فى استخدام فن بصمات الأصابع، لجأ المجرمون إلى ارتداء القفازات ومسح كل سطح مصقول أو ناعم لمسوه، وحينما استخدمت الشرطة أجهزة الراديو لإخطار سيارات النجدة الموجودة فى منطقة وقوع الجريمة لتوجيهها لتعقب الجناة، استخدم المجرمون أيضاً أجهزة الراديو أثناء أعمالهم وذلك لإخطار شركائهم بكافة البيانات التى تذيعها الشرطة عنهم. فهناك حرب تكنولوجية بين المجرمين وصناعة الأمن، فالمجرمون يسعون بشكل دائم نحو التغلب على التقدم التكنولوجى فى وسائل مكافحة الجريمة، كما أن تأثير الوسائل التكنولوجية التى تستخدم لحماية البنوك والمساكن وغيرها لمواجهة المنظمات الإجرامية قد يحد من نشاط تلك المنظمات، إلا أن هذا التأثير يكون لفترة قد تطول أو تقصر، ويتوقف البعد الزمنى لفاعليتها على مدى قدرة المنظمات الإجرامية على استخدام الوسائل التكنولوجية المضادة. وإذا كان المجرمون قد استفادوا من التطور التكنولوجى فى استحداث أساليب جديدة لارتكاب جرائمهم، **فإن الضرورة تقتضى وضع حدود جديدة للجريمة واستحداث أساليب جديدة لمكافحتها**[1]**، منها:**

1- السيد عوض: التطور التكنولوجى والجريمة، المؤتمر السنوى الرابع والثلاثون قضايا السكان والتنمية، 19-23 ديسمبر 2004، ص11.

1- حجب المواقع الإلكترونية المشبوهة التي تسعى إلى نشر الإرهاب والأفكار المتطرفة، وتلك المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين.

2- تفعيل الدور الوقائي الذي يسبق وقوع جريمة الإرهاب الإلكتروني، وذلـك مـن خلال تفعيل دور التعليم، وأجهزة الإعلام و التوعية من خلال (المسجد، الأسرة بخطورة هذه الجرائم على الأسرة والمجتمع، والسعي في تقوية الوازع الديني.

3- سن القوانين والتشريعات الخاصة التي تسد كافة الثغرات التي تكتنف جريمـة الإرهـاب الإلكتروني أو سبل التحقيق فيها، كالقوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية، وحفظها.

4- تنسيق وتوحيد الجهود بين الجهات المختلفة في الدولة: التشريعية، والقضائية، والضبطية، والفنية، وذلك مـن أجل سد منافذ جريمة الإرهاب الإلكتروني قدر المستطاع، والعمل على ضبطها وإثباتها بالطرق القانونية والفنية[1].

5- التوعية لكيفية الاستخدام والتشغيل الأمن للتكنولوجيا الحديثة العاملة على الإنترنت بالنسبة للمستخدمين ومسئولى نظم المعلومات ومزودى خدمة الدخول على شبكة الإنترنت.

6- رصد ميزانيات كافيةلتأمين أنظمة الاتصالات والمعلومات حيث أن النسبة المرصودة عالميا من 25% إلى 30% من إجمالى الميزانية المرصودة لإستخدام التكنولوجيا الحديثة.

7- وضع استراتيجيات واضحة لمعالجة مشكلة انخفاض أمن المعلومات عن طريق تحليل المخاطر المتمثلة فى التعرف على التهديدات التى يمكن أن تتعرض لها أنظمة هذه المعلومات[1].

1-http://www.assakina.com/book/71701.html تاريخ الدخول الثلاثاء إعداد المقدم د أيسر محمد عطيه 2016/6/28 2014

8- الرقابة من خلال الرصد والمراقبة والتحليل لكل مايبث عبر الشبكة والمحمول، وحاليا هناك فرق انشأتها العديد من الدول للمراقبة والتحليل فالجيش البريطاني لدية الفرقة 77، والصين لديها 2 مليون محلل لشبكة الانترنت، وكذلك تركيا واسرائيل لديها فرق تقوم بذلك.

9- الاختراق والتوجيه من خلال هويات مزيفة أو ما يطلق عليه جماهيريا في مصر اللجان أو المليشيات الإليكترونية. وتقوم بها أحيانا فرق متخصصة ومدربة بواسطة جهات حكومية (الصين - تركيا - اسرائيل) وهناك تجارب أجريت مؤخرا تستهدف الوصول إلي آليات تمكن من توجيه مشاعر وانطباعات مستخدمي الفيسبوك منها تجربة شاركت فيها جامعتا كورنيل وكاليفورنيا طبقت لمدة أسبوع عام 2012 علي 689 الف مستخدم دون علمهم أثارت سخطا وانتقادا داخل الولايات المتحدة وخارجها باعتبارها عملا غير أخلاقي ينتهك خصوصيات المستخدمين، واضطرت إدارة الفيسبوك للاعتذار.

10- الحجب للمواقع غير المرغوب فيها؛ حيث مازال هناك العديد من الحكومات المعادية للإنترنت التي تصر علي حجب العديد من المواقع والصحف الإلكترونية دون أحكام قضائية أو سند قانوني، أومنع خدمات وسائل الاتصال الحديثة من خلال العمل علي وقف خدمات رسائل الـSMS الجماعية، ووضع شروط كبيرة ومرهقة علي استخدامها. هذا بالإضافة إلي إقدام بعض الحكومات علي منع خدمات الهواتف الذكية بدعوي أنها تهدد الأمن القومي وتستخدم في التخابر لصالح دول أجنبية

1- على حسنى عباس: الاستخدام الأمن لشبكة الإنترنت وطرق الوقاية من مخاطر استخدامها، ورقة عمل،2010، ص5.

11- التوعية بأضرار ومغبة النشر غير المسئول علي الشبكة أو ما يطلق عليه محو الأمية المعلوماتية والرقمية Digital Literacy Information، وتعليم أخلاقيات التعامل مع وسائل الإعلام الجديد.

12- اكساب العاملين في الإعلام الجديد ثقافة إعلامية تتضمن القيم المهنية الإعلامية الرئيسية، مع اكساب العاملين في وسائل الإعلام التقليدية مهارات التعامل مع وسائل الإعلام الجديد.

13- وضع ضوابط أخلاقية تتمثل في مدونات سلوك تضعها المؤسسات الإعلامية الإلكترونية لإستخدام الانترنت ووسائل التواصل[1].

14- انشاء مركز للمعلومات الفضائية الرقمية لصد الإرهاب والمتسللين[2].

15- "ضرورة إنشاء مرصد يقوم عليه مجموعة من الباحثين المتخصصين لرصد الممارسات الإرهابية وصياغة برامج للأمن الفكري تتناسب مع الأوضاع المجتمعية والاقتصادية السائدة في الدولة".

16- "أن تكون إستراتيجية المواجهة للجماعات الإرهابية متعددة الأوجه تستعمل فيها الوسائل الأمنية والثقافية والتعبئة والإجراءات السياسية في خطة متكاملة"[3].

17- إعداد الكوادر الأمنية المؤهلة تأهيلاً إعلامياً، يمكنها من صياغة رسائل إعلامية واضحة ومؤثرة ذات مصداقية، كما أنّه من الواجب إطلاق مواقع دينية على مواقع التواصل الاجتماعي تخاطب الآخر وفق مفاهيم تقوم على مضامين انسانية راقية، وتعكس مفهوم الدين الإسلامي الحنيف كدين محبة وتعاون وسلام، مع إبراز

1- محمود علم الدين **وسائل التواصل الاجتماعي والأمن القومي**: جريدة أخبار اليوم، العدد 3749، 10 سبتمبر 2015.
2- جريدة الرأى: العدد13585، السبت 10 سبتمبر 2016.
3- السيد ياسين: المركز العربى للبحوث والدراسات، 10 سبتمبر 2016م.

الوجه المشرق للثقافة الإسلامية كوسيله لإغلاق الباب أمام تلك الجماعات التي تتخذ من الدين ستاراً للاختباء وراءه[1].

وتعد روسيا والصين والولايات المتحدة من أكبر القوى في مجال الإستحواذ على القوة الإلكترونية القادرة على توفير أقصى درجات الأمن الإلكتروني Cyber Security، وهو ما فرض على الدول وجود إجراءات حماية عبر تبني **سياسات دفاعية** تتضمن عمليات الحماية والتطوير لإجراءات الدفاع ضد الأخطار المحتملة وحماية نظم المعلومات ومنع تعرضها لعمليات هجومية معادية، وتعزيز الأمن الإلكتروني بأبعاده المتعلقة بالبرمجيات والبنية التحتية. ومنع استغلاله في الحرب النفسية. من أجل ضمان أمن وسلامة الفضاء الالكتروني، إلى جانب تبني **سياسات هجومية** في الفضاء الإلكتروني عبر اتخاذ إجراءات لمهاجمة مصادر التهديد وتعقب الفاعليين في الهجوم على منشآت البنية التحية الحيوية، ويتم استخدام نظم إلكترونية متقدمة كتطوير استخدام أسلحة إلكترونية في الحروب. ويشهد العالم تطورا حذرا وسريا في هذا الشأن.

ومن أبرز أنماط ممارسة القوة عبر الفضاء الإلكتروني "**نمط القوة الصلبة**" عبر استخدام مقدراته وأدواته في عمل تخريبي عبر قطع كابلات الاتصالات أو تدمير أنظمة الاتصالات أو الاقمار الصناعية أو استخدام الأسلحة الإلكترونية المتقدمة كالفيروسات في تدمير الانظمة المعلوماتية لمنشآت حيوية بشكل يؤثر على وظيفتها ويهدد امن الدولة والسكان.

وهناك نمط أخر لاستخدام القوة عبر الفضاء الإلكتروني فيما يمكن أن يطلق علية "**نمط القوة الناعمة**" وذلك بدعم دوره في إدارة العمليات النفسية والتأثير في الرأي العام وتكوين التحالفات الدولية وفي عمل أجهزة الاستخبارات الدولية بما وفره من سيل عالمى للمعلومات لا يقتصر علي وجهة النظر الرسمية للدول والحكومات, بل تعدي ذلك لدور الأفراد في إنتاج المعلومات وترويجها, وفي توافر كم هائل للتحليلات السياسية والاقتصادية مع تعدي الحدود الدولية وشكل ذلك ثورة

1- فايز الشهوي: الانترنت سلاح الارهاب الجديد، جريدة الرياض – العدد16985،25 ديسمبر 2014.

معلوماتية هائلة لا حدود لها, مادامت عكفت عليها أجهزة الاستخبارات الكبري للحصول عليها أولا, والبحث فيها ثانيا وتوظيف نتائجها ثالثا[1].

ولكن من الضرورى وأد الإرهاب قبل ظهوره، فالوقاية خيرا من العلاج لذا وجب على الدول بمختلف مؤسساتها وضع بعض الاستراتيجيات للقضاء على المناخ الذى ينمو فيه الإرهاب قبل أن يبدأ.

1- https://seconf.wordpress.com/15/05/2015/الفضاء-الإلكتروني مايو 15, 2015 مؤتمر حروب الفضاء السبرانى

سابع عشر: استراتيجيات الوقاية من الإرهاب الالكترونى.

1- الاستراتيجيات الاجتماعية والاقتصادية.

تتمثل فى تحسين الظروف الاقتصادية والاجتماعية والتى تشمل الفقر والأمراض والتهميش والبطالة والتى تضمن العيش الكريم لكل فئات المجتمع، حتى لا تنزلق فى دوامة الجماعات المتطرفة.

2- الاستراتيجيات السياسية.

فتح المجال لحرية الرأى والتعبير، وتوفر مبدأ تداول السلطة مما يساعد مختلف القوى على من تشكيل أنفسها فى منظومات سياسية تعبر عن توجهاته الفكرية.

3- الاستراتيجيات القانونية.

عن طريق بعض الإصلاحات التى أدخلتها أغلبية المجتمعات لحماية الأجهزة الرقابية من الأفات الخطيرة التى أصبحت تتكاثر بسرعة مذهلة مثل تبييض الأموال، وتجارة الأعضاء، والجريمة المنظمة والنشطات الإرهابية وغيرها[1].

4- الاستراتيجيات الإعلامية.

من خلال تجنيد كل وسائل الإعلام المسموعة والمرئية والمكتوبة فى شرح ماهية الإرهاب وأهدافه وتوجهاته وأثره على تطور المجتمعات، مما يقلص من الأثر الذى تحدثه المرجعيات الثقافية والدينية التى تعتمد عليها الجماعات الإرهابية فى تجنيد الأفراد وتبرير نشاطتها.

1- إبراهيم محمد جاسم: المواجهة العلمية فى مواجهة الارهاب فى الشبكات الاجتماعية، دورة تدريبية فى الفترة من 23-2013/2/27م، ص10

5- الاستراتيجيات الأمنية.

والتى تتجسد فى تطوير وتحديث النظام المعلوماتى واللوجيستى للأجهزة الأمنية مما يمكنها من إحداث الضرر بالجماعات المتطرفة عن طريق إجهاض الكثير من العمليات الإرهابية.

ولكن ليس كافيا أن تقوم كل دولة تواجه الإرهاب بسبل المكافحة سالفة الذكر، فالارهاب جريمة أصبحت منتشرة فى العالم كله، والإرهاب الالكترونى جريمة عابرة القارات لذا فمواجهتها تحتاج إلى تكاتف للجهود الدولية لوأد هذه الظاهرة التى تهدد أمن وسلامة المجتمعات بل تهدد كيانها وبقاءها.

ثامن عشر: الجهود الدولية لمكافحة الارهاب الإلكترونى:

الإرهاب أصبح خطر دولي يؤرق كل المجتمعات لذلك وجب على المجتمعات الدولية التكاتف من أجل مواجهة الإرهاب الذى سيقضى على العالم بأثره:

1- مراجعة الإتفاقيات والمعاهدات الدولية الخاصة بتقنية المعلومات والاتصالات وتضمين صور الجريمة الالكترونية وعقوبتها في بنود الاتفاقيات والمعاهدات الدولية[1].

2- ايجاد منظومة قانونية دولية تحت مظلة الأمم المتحدة يعهد إليها توثيق وتوحيد جهود الدول في مكافحة ومواجهة الارهاب الالكتروني، ويتفرع منها جهة أو هيئة محايدة تتولى التحقيق فى هذه الجرائم، ويكون لها سلطة الأمر بضبط وإحضار المجرم للتحقيق معه أي كان مكان وجوده وجنسيته وبلده.

3- عقد الاتفاقيات بين الدول بخصوص جرائم الإرهاب الالكتروني وتنظيم كافة الإجراءات المتعلقة بالوقاية من هذه الجريمة وعلاجها وتبادل المعلومات والأدلة في شأنها بما في ذلك تفعيل اتفاقيات تسليم الجناة في جرائم الإرهاب الالكتروني.

4- تعزيز التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية التخريبية الإلكترونية الواقعة في أراضيها ضد دول أو جهات أخرى خارج هذه الأراضي[2].

1- جريدة الرأى، العدد 13585 السبت 10 سبتمبر 2016.

2-http://www.assakina.com/book/71701.html تاريخ الدخول الثلاثاء إعداد المقدم د أيسر محمد عطيه 2016/6/201428.

5- سن القوانين والتشريعات الدولية لإمكانية تتبع الإرهابين وملاحقتهم خاصة وأن الإرهاب الإلكترونى أحد أشكال الجريمة الإلكترونية التى تتسم بأنها جريمة عابرة القارات.

نماذج فعلية للجهود الدولية التى تمت فى الواقع لمواجهة الإرهاب الإلكترونى.

ا- اتفاقية عام 1988 والتى حثت دول العالم على الدخول فى اتفاقيات ثنائية ضد الإرهاب الإلكترونى.

2- فى عام 2000 صدرت مسودة إتفاق عالمى حول الجريمة والارهاب الإلكترونى من جامعة استانفورد فيما عرف بخطة ستانفورد وشملت تلك الخطة العديد من النقاط حول هدف الوصول إلى تعاون دولى أوسع فى مقاومة هجمات الفضاءالإلكترونى، وذلك على اعتبار أن الإرهابيين والمجرمين يستغلون نقاط الضعف فى القوانين، وخاصة مع التطور المستمر فى التكنولوجيا وجمود الأطر القانونية الحالية فى مواجهة الأخطار والهجمات، وفى المادة 12 من تلك الخطة اقتراح بإقامة وكالة دولية لحماية البنية التحتية الكونية للمعلومات[1].

ولكن مع كل سبل المكافحة السابق ذكرها يبقى رصد جرائم الارهاب الإلكترونية صعبا للغاية وذلك للأسباب الأتية:

1- رائد العدوان: المعالجة الدواية لقضايا الإرهاب الإلكترونى،دورة تدريبية فى الفترة من 23-2003/2/27، ص9- 10.

تاسع عشر: صعوبة اكتشاف جرائم الإرهاب الإلكتروني:

1- عدم كفاية القوانين لمواجهة التنامى المتزايد بسرعة فى الصور المستحدثة من هذه الجرائم.

2- سهولة القيام بإخفاء معالم الجريمة فى عدم معرفة مصدر مرتكب الفعل.

3- وجود كم كبير من المعلومات يتعين فحصها،والتى يكون لها ارتباط بمعلومات خاصة بارتكاب الجريمة،وتعتبر المعلومات داخل الجهاز دليلا تسعى الجهات الأمنية لملاحقته. وهو أمر يتسم بكثير من الصعوبات إما بسبب طبيعة المعلومات المتاحة أو نقص الخبرة الفنية من قبل رجال الأمن فى ملاحقتهم لتلك الأدلة مما يتطلب مع البحث استغراق فترة زمنية تؤثر بالسلب على طبيعة عمل المنشأة[1].

4- أغراضها متعددة وحجم الخسائر الناجمة عنها خطير مقارنة بالجرائم التقليدية مثل تفجير الطائرة الروسية فهو يمثل ضربة للسياحة المصرية وضرب للعلاقات المصرية الروسية، وإعطاء صورة عن انتشار الارهاب فى مصر وعدم قدرها على السيطرة عليه،وضعف الأمن بها،هذا بالاضافة إلى الخسائر فى الأرواح.

5- مرتكبها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمرا صعبا[2].

1- رامى متولى: الجرائم المعلوماتية وطرق مواجهتها، ورقة عمل مؤتمر تأمين المعلومات والدليل الرقمى وكيفية إثباته فى الجرائم الإلكترونية (15- 16 ديسمبر 2010) المركز القومى للبحوث الاجتماعية والجنائية ص8.

2- أحمد محمد أمين الشريف: الجرائم المستحدثة عبر الإنترنت فى مجال حماية الأداب العامة، ورقة عمل الادارة العامة لحماية الأداب، ص9.

الفصل الثالث

نتائج الدراسة الميدانية

"حول اتجاهات الشباب بالجامعات المصرية نحو الجريمة الإلكترونية"

نتائج الدراسة الميدانية ومناقشتها

نتائج دراسة تم تطبيقها على عينة من شباب الجامعة ببعض الجامعات المصرية لقياس اتجاهاتهم نحو الجريمة الإلكترونية:

جدول (1)

فى رأيك الجريمة الإلكترونية جريمة ترتكب عن طريق الكمبيوتر

النوع / الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	17	8.6	19	9.8	36	9.2
أحيانا	86	43.7	77	39.9	163	41.8
نعم	94	47.7	97	50.3	191	49.0
الإجمالي	**197**	**100**	**193**	**100**	**390**	**100**

قيمة كا^2 = 61. **درجة الحرية = 2** **مستوى المعنوية= 763.**

تدل بيانات الجدول السابق على:

(49.0%) من الشباب عينة الدراسة يرون أن الجرائم الإلكترونية ترتكب بواسطة الكمبيوتر موزعة بنسبة (47.7%) للذكور فى مقابل (50.3%) للإناث ويشير ذلك إلى معرفة الشباب للجريمة الإلكترونية وسبل ارتكابها وقد يرجع ارتفاع نسبة الإناث الذين أشاروا إلى ارتكاب الجريمة بواسطة الكمبيوتر عن الذكور غلى ارتفاع نسبة مشاهدة الإناث للدراما الاجنبية المقدمة للجريمة الإلكترونية متفوقة بذلك على الإناث وفق لما أشارت إليه نتائج الجدول رقم (7/أ) بهذه الدراسة، بينما (41.8.%) من الشباب عينة الدراسة يرون ان الجريمة الإلكترونية ترتكب أحيانا عن طريق الكمبيوتر موزعة بنسبة (43.7%) للذكور فى مقابل (39.9%) للإناث وهذا يشير إلى عدم وعى عدد من العينة بالجريمة الإلكترونية وسبل ارتكابها مما قد يجعلهم إما ضحية لمرتكبى هذه الجرائم أو هم أنفسهم مرتكبين لهذه الجريمة عن دون وعى

منهم بذلك مما قد يعرضهم للمسائلة القانونية، بينما نجد أن (9.2%) من الشباب عينة الدراسة يرون أنه لا ترتكب الجريمة الإلكترونية بواسطة الكمبيوتر موزعة بنسبة (8.6%) للذكور فى مقابل (9.8%) للإناث.

إجمالى نتائج الجدول تشير إلى ارتفاع نسبة الشباب عينة الدراسة ممن لديهم الوعى بالجريمة الإلكترونية وسبل ارتكابها.

جدول (2)
اعتقاد الشباب حول احتواء الجريمة الإلكترونية على عنف

النوع / الاعتقاد	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	59	29.5	44	22.0	103	25.8
أحياناً	97	48.5	101	50.5	198	49.5
نعم	44	22.0	55	27.5	99	24.8
الاجمالى	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 = 3.48 **درجة الحرية = 2** **مستوى المعنوية= 175.**

تدل بيانات الجدول السابق على:

أن(49.5%) من الشباب عينة الدراسة يعتقدون ان الجريمة الإلكترونية ان أحيانا ما يكون بها عنف موزعة بنسبة (48.5%) للذكور فى مقابل (50.5%) للإناث وقد يرجع ذلك إلى اعتقادهم إلى أن الجريمة جريمة بغض النظر عن طرق ارتكابها، بينما (25.8%) موزعة بنسبة (29.5%) للذكور فى مقابل (22.0%) للإناث من الشباب عينة الدراسة يرون أن الجريمة الإلكترونية ليس بها عنف وقد يرجع ذلك إلى تأثرهم بطريقة ارتكاب الجريمة الإلكترونية بواسطة الحاسب، فى حين يرى (24.8%) من الشباب عينة الدراسة يعتقدون أن الجريمة الإلكترونية بها عنف موزعة بنسبة (22.0%) للذكور فى مقابل (27.5%) للإناث.

جدول (3)

ارتكاب الجريمة الالكترونية فى بعض الاحيان دون قصد

النوع / الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	40	20.0	35	17.5	75	18.8
أحياناً	37	18.5	21	10.5	58	14.5
نعم	123	61.5	144	72.0	267	66.8
الاجمالى	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 = 6.39　　　درجة الحرية = 2　　　مستوى المعنوية= 041.

تدل بيانات الجدول السابق على:

أن (66.8%) من الشباب عينة الدراسة موزعة بنسبة (61.5%) للذكور فى مقابل (72.0%) للإناث يرون ان الجريمة الإلكترونية ترتكب دون قصد ويعكس ذلك عدم الوعى الكافى لدى الشباب بالجريمة الإلكترونية وهذا يعنى أنهم قد يرتكبوا الجريمة دون قصد ،بينما (18.8%) من الشباب عينة الدراسة موزعة بنسبة (20.0%) للذكور فى مقابل (17.5%) للإناث يرون أن الجريمة الإلكترونية يرتكب بقصد وقد يرجع ذلك إلى اعتقادهم بأن الجريمة لابد وأن يكون لها هدف وأسباب محددة ومرتكب وضحية فهى لاتكون إلا عن قصد، فى حين أن(14.5%) من الشباب عينة الدراسة موزعة بنسبة (18.5%) للذكور فى مقابل (10.5%) للإناث يرون أن الجريمة الإلكترونية أحيانا ما ترتكب دون قصد.

جدول (4)

أراء الشباب حول الجرائم الإلكترونية التى يرتكبها الفرد دون أن يعى أنها جريمة

النوع / الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
تدمير بعض الملفات دون إذن صاحبها	29	18.1	25	15.2	54	16.6
نسخ بعض الملفات دون وجه حق	28	17.5	36	21.8	64	19.7
تحميل بعض الأغانى والأفلام من الانترنت	27	16.9	32	19.4	59	18.2
جميع ماسبق	76	47.5	72	43.6	148	45.5
الاجمالى	**160**	**100**	**165**	**100**	**325**	**100**

قيمة كا^2 = 1.752 درجة الحرية = 3 مستوى المعنوية=.626..غير دالة

تدل بيانات الجدول السابق على:

أن (45.5%) من الشباب عينة الدراسة موزعة بنسبة (47.5%) للذكور فى مقابل (43.6%) للإناث يرون أن جميع الجرائم الموجودة بالجدول سابق هى جرائم إلكترونية يرتكبها الفرد عينة الدراسة دون أن يعى أنها جريمة ويعكس ذلك وعى الشباب عينة الدراسة بالجرائم الإلكترونية وبعض أشكالها وقد يحميهم ذلك من ارتكاب مثل هذه الجرائم، بينما يرى (19.7%) من الشباب موزعة بنسبة (17.5%) للذكور فى مقابل (21.8%) للإناث أن لنسخ بعض الملفات دون وجه حق تمثل الجريمة التى يرتكبها الفرد دون أن يعى أنها جريمة، بينما يرى (18.2%) من الشباب موزعة بنسبة (16.9%) للذكور فى مقابل (19.4%) للإناث أن **تحميل بعض الأغانى والأفلام من الانترنت تمثل الجريمة التى يرتكبها الفرد دون أن يعى أنها جريمة،** فى حين يرى(16.6%) من الشباب موزعة بنسبة (18.1%) للذكور فى مقابل (15.2%) للإناث أن **تدمير بعض الملفات دون إذن صاحبها** .

تمثل الجريمة التى يرتكبها الفرد دون أن يعى أنها جريمة وهذا يعكس أن أكثر من نصف عينة الدراسة قد ترتكب الجرائم الأخرى دون أن تعى أنها جريمة.

جدول (5)

الاعتقاد فى أنه كلما زاد الاعتماد على الوسائل التكنولوجية الحديثة كلما زاد حجم الجريمة الإلكترونية

النوع الاعتقاد	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	22	11.0	21	10.5	43	10.8
أحياناً	52	26.0	53	26.5	105	26.3
نعم	123	61.5	126	63.0	249	62.3
لا أعرف	3	1.5	-	-	3	8.0
الاجمالى	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 = 3.069 درجة الحرية = 3 مستوى المعنوية= 381. غير دالة

تدل بيانات الجدول السابق على:

أن (62.3%) من الشباب عينة الدراسة موزعة بنسبة (61.5%) للذكورفى مقابل (63.0%) للإناث يعتقدون أنه كلما زاد الاعتماد على الوسائل التكنولوجية الحديثة كلما زاد حجم الجريمة الإلكترونية وهذا قد يشير إلى وعى الشباب عينة الدراسة بأن الوسائل التكنولوجية الحديثة كما لها مزايا عليها الكثير من العيوب والمشاكل، بينما يرى (26.3%) من الشباب موزعة بنسبة (26.0%) للذكور فى مقابل (26.5%) للإناث يعتقدون أنه أحيانا كلما زاد الاعتماد على الوسائل التكنولوجية الحديثة كلما زاد حجم الجريمة الإلكترونية، بينما يرى (10.8%) من الشباب موزعة بنسبة (11.0%) للذكور فى مقابل (10.5%) للإناث يعتقدون أنه ليس بالضرورة كلما زاد الاعتماد على الوسائل التكنولوجية الحديثة كلما زاد حجم الجريمة الإلكترونية، فى حين أن (8.%) من الشباب موزعة بنسبة (1.5%) للذكور فى مقابل لا شىء للإناث لايعرفون ما إذا كاننت زيادة الاعتماد على الوسائل التكنولوجية الحديثة يؤدى إلى زيادة حجم للجريمة الالكترونية وهذا يعكس أنهم قد يكونوا عرضة لمخاطر التكنولوجيا الحديثة ومنها الجريمة الإلكترونية.

جدول (6)

اعتقاد الشباب حول الفرق بين الجريمة الإلكترونية والجريمة التقليدية

النوع الاعتقاد	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	15	7.5	15	7.5	30	7.5
أحياناً	16	8.0	17	8.5	33	8.3
نعم	169	84.5	168	84.0	337	84.3
الاجمالى	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا2 =.033 درجة الحرية= 2 مستوى المعنوية= .984غير دالة

تدل بيانات الجدول السابق على:

أن (84.3%) من الشباب عينة الدراسة موزعة بنسبة (84.5%) للذكور فى مقابل (84.0%) للإناث يعتقدون أن هناك فرق بين الجريمة الإلكترونية والجريمة التقليدية وهذا قد يشير إلى معرفة الشباب عينة الدراسة بالجريمة الإلكترونية وطرق ارتكابها، بينما يرى (8.3%) من الشباب موزعة بنسبة (8.0%) للذكور فى مقابل (8.5%) للإناث يعتقدون أنه أحيانا يكون هناك فرق بين الجريمة الإلكترونية والجريمة التقليدية، بينما يرى (7.5%) من الشباب موزعة بنسبة (7.5%) للذكور فى مقابل (7.5%) للإناث يعتقدون أنه ليس فرق بين الجريمة الإلكترونية والجريمة التقليدية وهذا قد يرجع إلى أحد أمرين الأول اعتبار عدم الفرق بينهما نابعا من أن كلاهما جريمة لها أهدافها وأسبابها ومرتكبيها وضحاياها، والأمر الأخر هو عدم معرفتهم بالجريمة الإلكترونية ولا طرق ارتكابها.

جدول رقم (7)

الفرق بين الجريمة الإلكترونية والجريمة التقليد ية

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
الجريمة الإلكترونية مرتكبها ليس مجرم بطبعه عكس الجريمة التقليدية	63	34.1	59	31.9	122	33.0	.442	غير دالة
الجريمة الإلكترونية لا يسهل التوصل لمرتكبها عكس الجريمة التقليدية	45	24.3	44	23.8	89	24.1	.121	غير دالة
الجريمة الإلكترونية لا يصحبها عنف عكس الجريمة التقليدية	38	20.5	48	25.9	86	23.2	1.229	غير دالة
الجريمة الإلكترونية عابرة الحدود عكس الجريمة التقليدية	33	17.8	32	17.3	65	17.6	.136	غير دالة
الجريمة الإلكترونية تحتاج إلى حاسب إلى لإرتكابها عكس الجريمة التقليدية	23	12.4	39	21.1	62	16.8	2.224	دالة 0.05
الجريمة الإلكترونية يصعب إثباتها عكس الجريمة التقليدية	37	20.0	44	23.8	81	21.9	.879	غير دالة
جميع ما سبق	63	34.1	60	32.4	123	33.2	.331	غير دالة
جملة من سئلوا	**185**		**185**		**370**			

أوضحت بيانات الجدول السابق أراءالشباب حول الفرق بين الجريمة الإلكترونية والجريمة التقليدية والتى جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاءت جميع ما سبق من فروق بالجدول فى مقدمة الفروق بين الجريمة الإلكترونية والتقليدية بنسبة بلغت (33.2%)، موزعة بنسبة (34.1%) للذكور فى مقابل (32.4%) للإناث. بينما جاء فى الترتيب الثانى فى **الفرق بين الجريمة الإلكترونية والجريمة التقليدية أن الجريمة الاإلكترونية مرتكبها ليس مجرم**

بطبعه عكس الجريمة التقليدية بنسبة بلغت (33.0%)، موزعة بنسبة (34.1%) للذكور فى مقابل (31.9%) للإناث. بينما جاء فى الترتيب الثالث فى **الفرق بين الجريمة الإلكترونية والجريمة التقليدية أن الجريمة الإلكترونية لا يسهل التوصل لمرتكبها عكس الجريمة التقليدية** بنسبة بلغت (24.1%)، موزعة بنسبة (24.3%) للذكور فى مقابل (23.8%) للإناث. بينما جاء فى الترتيب الرابع فى **الفرق بين الجريمة الإلكترونية والجريمة التقليدية أن الجريمة الإلكترونية لا يصحبها عنف عكس الجريمة التقليدية** بنسبة بلغت (23.2%)، موزعة بنسبة (20.5%) للذكور فى مقابل (25.9%) للإناث. بينما جاء فى الترتيب الخامس **الفرق بين الجريمة الإلكترونية والجريمة التقليدية أن الجريمة الإلكترونية يصعب إثباتها عكس الجريمة التقليدية** بنسبة بلغت (21.9%)، موزعة بنسبة (20.0%) للذكور فى مقابل (23.8%) للإناث. بينما جاء فى الترتيب السادس **الفرق بين الجريمة الإلكترونية والجريمة التقليدية أن الجريمة الإلكترونية عابرة الحدود عكس الجريمة التقليدية** بنسبة بلغت (17.6%)، موزعة بنسبة (17.8%) للذكور فى مقابل (17.3%) للإناث.. بينما جاء فى الترتيب السابع **الفرق بين الجريمة الإلكترونية والجريمة التقليدية أن الجريمة الإلكترونية تحتاج إلى حاسب إلى لإرتكابها عكس الجريمة التقليدية** بنسبة بلغت (16.8%)، موزعة بنسبة (12.4%) للذكور فى مقابل (21.1%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحصائيا بين الذكور والإناث حول الفرق بين الجريمة الإلكترونية والجريمة التقليدية والتى جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

- تزداد نسبة الإناث ممن يرون **أن الفرق بين الجريمة الإلكترونية والجريمة التقليدية أن الجريمة الإلكترونية تحتاج إلى حاسب إلى لإرتكابها عكس الجريمة التقليدية** عن الذكور بنسبة (21.1%) (12.4%)، على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(2.224) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%). هذه النتيجة قد

تعكس أحد أمرين إما وعى الشباب الإناث بالجريمة الإلكترونية وإما ضيق أفق العينة لدرجة تصل إلى حد اختصار الفروق الكثيرة بين الجريمة الإلكترونية والجريمة التقليدية فى هذا الفرق.

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث حول الفرق بين الجريمة الإلكترونية والجريمة التقليدية والتى جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

- يتقارب نسبة الشباب الذكور والإناث فى اعتبار **الفرق بين الجريمة الإلكترونية والجريمة التقليدية يتمثل فى** جميع ما سبق من فروق بالجدول بنسبة بلغت (33.2%)، (34.1%) على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.302) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث فى اعتبار **الفرق بين الجريمة الإلكترونية والجريمة التقليدية يتمثل فى أن الجريمة الإلكترونية مرتكبها ليس مجرم بطبعه عكس الجريمة** (34.1%)، (31.9%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (442.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث فى اعتبار **الفرق بين الجريمة الإلكترونية والجريمة التقليدية يتمثل فى أن الجريمة الإلكترونية لا يسهل التوصل لمرتكبها عكس الجريمة التقليدية** (24.3%)، (23.8%) للإناث على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (121.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث فى اعتبار**الفرق بين الجريمة الإلكترونية والجريمة التقليدية يتمثل فى أنلا يصحبها عنف عكس الجريمة التقليدية** (20.5%)، (25.9%). على الترتيب.والفارق غير دال إحصائيا حيث بلغت

قيمة Z المحسوبة 1.229 وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث فى اعتبار**الفرق بين الجريمة الإلكترونية والجريمة التقليدية يتمثل فى أن الجريمة الإلكترونية يصعب إثباتها عكس الجريمة التقليدية** (20.0%)، (23.8%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (879.)وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث فى اعتبار**الفرق بين الجريمة الإلكترونية والجريمة التقليدية يتمثل فى أن الجريمة الإلكترونية عابرة الحدود عكس الجريمة التقليدية** (17.8%)، (17.3%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (136.)وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

جدول (8)
اعتقاد الشباب حول إمكانية وجود أهداف مشروعة للجريمة الإلكترونية

النوع	ذكور		إناث		الإجمالي	
مدى الاعتقاد	ك	%	ك	%	ك	%
لا	106	53.0	107	53.5	213	53.3
أحياناً	54	27.0	58	29.0	112	28.0
نعم	40	20.0	35	17.5	75	18.8
الاجمالى	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =.786 درجة الحرية = 2 مستوى المعنوية=.481غير دالة

تدل بيانات الجدول السابق على:

أن (53.3%) من الشباب عينة الدراسة موزعة بنسبة (53.0%) للذكور فى مقابل (53.5%) للإناث يعتقدون أنه لا يوجد أهداف مشروعة للجريمة الإلكترونية وقد يرجع ذلك إلى رؤيتهم للجريمة على أنها جريمة لها أضرارها وضحاياها بصرف النظر عن الهدف منها، بينما يرى (28.0%) من الشباب موزعة بنسبة (27.0%) للذكور فى مقابل (29.5%) للإناث يعتقدون أنه أحيانا ما يكون للجريمة الإلكترونية أهداف مشروعة،فى الوقت الذى يرى فيه (18.8%) من الشباب موزعة بنسبة (20.0%) للذكور فى مقابل (17.5%) للإناث يعتقدون فى أن هناك أهداف مشروعة للجريمة الإلكترونية .

تأسيساً على ما سبق يتضح أنه لا يوجد فروق ذات دلالة إحصائية بين طلاب الجامعات في إمكانية وجود أهداف مشروعة للجريمة الإلكترونية، حيث كانت قيمة كا2 = وهي غير دالة .

جدول (9)

أراء الشباب حول أسباب عدم وجود أهداف مشروعة للجريمة الإلكترونية

النوع / الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لأن الجريمة جريمة أيا كان أهدافها	5	42.5	45	42.1	90	42.3
لأن مرتكبها مجرم فكيف يفعل أشياء إيجابية	8	7.5	48	16.8	26	12.2
لأنها تسبب الضرر للآخرين	43	40.6	37	34.6	80	37.6
أخرى.	10	9.4	7	6.5	17	8.0
جملة من سئلو	**106**	**100**	**107**	**100**	**213**	**100**

قيمة كا^2 = 4.821 درجة الحرية = 3 مستوى المعنوية= غير دالة185.

تدل بيانات الجدول السابق على:

أن (42.3%) من الشباب عينة الدراسة موزعة بنسبة (42.5%) للذكور فى مقابل (42.1%) للإناث يرون أنه لا يوجد أهداف مشروعة للجريمة الإلكترونية لأن الجريمة جريمة أيا كان هدفها، بينما يرى (37.6%) من الشباب موزعة بنسبة (40.6%) للذكور فى مقابل (34.6%) للإناث يرون أن عدم وجود أهداف مشروعة للجريمة الإلكترونية يرجع إلى أنها تسبب الضرر للأخرين، فى الوقت الذى يرى فيه (12.2%) من الشباب موزعة بنسبة (7.5%) للذكور فى مقابل (16.8%) يرون أن الجرائم الإلكترونية ليس لها أهداف مشروعة لأن مرتكبها مجرم فكيف يفعل أشياء إيجابية بينما يرى (8.0%) من الشباب أسباب أخرى غير المذكورة ولكن لم تفصح عنها العينة.

تأسيسًا على ما سبق يتضح أنه لا يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب حول أسباب عدم وجود أهداف مشروعة للجريمة الإلكترونية.

جدول (10)

أراء الشباب حول أى من هذه الأفعال لا يعتبر جريمة إلكترونية

النوع / الرأى	ذكور ك	ذكور %	إناث ك	إناث %	الإجمالي ك	الإجمالي %
.الترويج لمواقع إباحية	9	4.5	8	4.0	17	4.3
ننشر بعض الصور والتعليقات على الفيس بوك	142	71.0	152	76.0	294	73.5
تحميل بعض المواد من الإنترنت دون ترخيص.	27	13.5	14	7.0	41	10.3
الدخول على مواقع القمار	9	4.5	10	5.0	19	4.8
سب وقذف الآخرين على الانترنت	7	3.5	8	4.0	15	3.8
التشهير بالآخرين على الإنترنت	6	3.0	8	4.0	14	3.5
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 = 4.926   درجة الحرية = 5   مستوى المعنوية= 425.غير دالة

تدل بيانات الجدول السابق على:

أن (73.5%) من الشباب عينة الدراسة موزعة بنسبة (71.0%) للذكور فى مقابل (76.0%) للإناث أن **ننشر بعض الصور والتعليقات على الفيس بوك** لا يعتبر جريمة إلكترونية وهذا قد يعكس معرفة الشباب بالجريمة الإلكترونية وأى الأفعال يعتبر أمر عادى وأيها يدخل فى إطار الجريمة، بينما (10.3%) من الشباب عينة الدراسة موزعة بنسبة (13.5%) للذكور فى مقابل (7.0%) للإناث أن **تحميل بعض المواد من الإنترنت دون ترخيص** لا يعتبر جريمة إلكترونية، فى حين أن (4.8%) من الشباب عينة الدراسة موزعة بنسبة (4.5%) للذكور فى مقابل (5.0%) للإناث أن**الدخول على مواقع القمار** لا يعتبر جريمة إلكترونية، **بينما** (4.3%) من الشباب عينة الدراسة موزعة بنسبة (4.5%) للذكور فى مقابل (4.0%) للإناث أن **الترويج لمواقع إباحية** لا يعتبر جريمة إلكترونية، **بينما** (3.8%) من الشباب عينة الدراسة موزعة بنسبة (3.5%) للذكور فى مقابل (4.0%) للإناث أن **سب وقذف الآخرين على الانترنت** لا يعتبر جريمة إلكترونية، فى الوقت الذى يرى فيه (3.5%) من الشباب

موزعة بنسبة (3.0%) للذكور فى مقابل (3.5%) للإناث أن **التشهير بالآخرين على الإنترنت** لا يعتبر جريمة إلكترونية وقد تشير هذه النتيجه إلى أمكانية ارتكاب الشباب لهذه الجرائم دون أن يعرف انها جريمة يعاقب عليها القانون.

تأسيساً على ما سبق يتضح أنه لا يوجد فروق ذات دلالة إحصائية بين الجامعات فى معرفة الشباب بالأفعال التى تشكل جرائم إلكترونية، حيث كانت قيمة كا2 = وهي غير دالة .

جدول (11)

هل تعتقد أنه يوجد جرائم إلكترونية فى مصر ؟ * النوع

النوع / الاعتقاد	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	-	-	5	2.5	5	1.3
أحياناً	14	7.0	15	7.5	29	7.3
نعم	168	.84	142	71.0	310	77.5
لا أعرف	18	9.0	38	19.0	56	14.0
اجمالى	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 = 14.358 درجة الحرية = 3 مستوى المعنوية =. 002 دالة

تدل بيانات الجدول السابق على:

أن (77.5%) من الشباب عينة الدراسة موزعة بنسبة (84.0%) للذكور فى مقابل (71.0%) يعتقدون فى وجود جرائم الالكترونية مصر وقد تعكس هذه النتيجة معرفة الشباب بالجرائم الإلكترونية ومعاناة المجتمع المصرى منها كغيرها من الشباب، بينما(14.0%) من الشباب عينة الدراسة موزعة بنسبة (9.0%) للذكور فى مقابل (19.0%) لايعرفون ما إذا كان هناك جرائم إلكترونية فى مصرفى حين أن (7.3%) من الشباب عينة الدراسة موزعة بنسبة (7.0%) للذكور فى مقابل (7.5%) يعتقدون أنه أحيانا يوجد جرائم الالكترونية فى مصر، فى الوقت الذى يرى فيه (1.3%) من الشباب عينة الدراسة موزعة بنسبة (2.5%) للإناث فى مقابل لا شىء للذكور يعتقدون أنه لا وجود للجرائم الالكترونية فى مصروقد ترجع ذلك إلى عدم تعرضهم الكافى لوسائل الاعلام أو عدم تعرضهم لللجريمة الإلكترونية او مصادفتهم لأحد من مرتكبيها.

تأسيساً على ما سبق يتضح أنه يوجد فروق ذات دلالة إحصائية بين االنوع والاعتقاد فى وجود جرائم إلكترونية فى مصر عند 0.01.

جدول رقم (12)

مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
تشاهد نماذج منها بالدراما الأجنبية	85	46.7	98	62.4	183	54.0	2.891	دالة**
تشاهد بعض الشباب يقومون به	69	37.9	41	26.1	110	32.4	2.310	دالة*
حملات التوعية التى تنظمها الكلية بشأن هذه الجرائم	16	8.8	13	8.3	29	8.6	.167	غير دالة
صادفت بعض الأفراد تعرضوا إليها	50	27.5	34	21.7	84	24.8	1.235	غير دالة
تقوم بإرتكابها	15	8.2	5	3.2	20	5.9	1.968	دالة*
أخرى	11	6.0	6	3.8	17	5.0	.933	غير دالة
جملة من سئلوا	**182**		**157**		**339**			

أوضحت بيانات الجدول السابق مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

مشاهدة نماذج من الجريمة الإلكترونية بالدراما الأجنبية فى مقدمة **مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر** بنسبة بلغت (54.7%)، موزعة بنسبة (46.7%) للذكور فى مقابل (62.4%) للإناث. بينما جاء فى الترتيب الثانى مشاهدة بعض الشباب يقومون بها بنسبة بلغت (32.4%)، موزعة بنسبة (37.9%) للذكور فى مقابل (26.1%) للإناث. بينما جاء فى الترتيب الثالث مصادفة بعض الأفراد تعرضوا إليها بنسبة بلغت (24.8%)، موزعة بنسبة (27.5%) للذكور فى مقابل (21.7%) للإناث. بينما جاء فى الترتيب الرابع حملات التوعية التى تنظمها الكليه بشأن هذه الجرائم بنسبة بلغت (8.6%)، موزعة بنسبة (8.8%) للذكور فى مقابل (8.3%) للإناث، بينما جاء فى الترتيب الخامس تقوم بإرتكابها بنسبة بلغت (5.9%)، موزعة بنسبة (8.2%) للذكور فى مقابل (3.2%) للإناث، بينما جاء فى

الترتيب وأسباب أخرى لم تفصح عنها العينة بنسبة بلغت (5.8%) لكل منهم، بينما جاء فى الترتيب السابع لأنه ليس بها عنف بنسبة بلغت (5.0%)، موزعة بنسبة (6.0%) للذكور فى مقابل (3.8%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحصائيا بين الذكور والإناث في مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر على النحو الأتى:

- تزداد نسبة الذكور في مصادر معرفتهم بوجود جرائم إلكترونية فى مصر على مشاهدة بعض الشباب يقومون بها عن الإناث بنسبة بلغت (37.9%)، (32.4%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة (2.310) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%). وقد يرجع ذلك إلى أن الذكور مرتكبى هذه الجرائم يتسمون بالجرأة عن الإناث فقد ينتاب الإناث الخوف من ارتكاب مثل هذه الجرائم خوفا من الوقوع تحت طائلة القانون أما الذكور فالرغبة لديهم فى إثبات الذات قد تجعلهم يفعلون ذلك .
- تزداد نسبة الإناث في مصادر معرفتهم بوجود جرائم إلكترونية فى مصر على مشاهدة نماذج منها بالدراما الأجنبية عن الذكور بنسبة (62.4%)، (46.7%)،على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة (2.891) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (99%).
- تزداد نسبة الذكور **في مصادر معرفتهم بوجود جرائم إلكترونية فى مصر على قيامهم بإرتكابها عن الإناث** بنسبة بلغت (8.2%)، (3.2%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.968) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%). وقد يرجع ذلك إلى أن الذكور مرتكبى هذه الجرائم يتسمون بالجرأة عن الإناث إلى جانب طبيعة الذكور القوية الجامدة وحب المغامرة لديهم عكس طبيعة الإناث الضعيفة الرقيقة.

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث في مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر على النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث فى **مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر** من خلال حملات التوعية التى تنظمها الكلية بشأن هذه الجرائم بنسبة بلغت (8.8%)، (8.3%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (.176) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث فى **مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر** من خلال مصادفة بعض الأشخاص الذين تعرضوا إليها بنسبة بلغت (27.5%)، (21.7%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.235) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث فى **مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر** من خلال مصادر اخرى غير الذكورة بالجدول لم تفصح عنها العينة بنسبة بلغت (6.0%)، (3.8%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (.933) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين بمستوى ثقة (95%).

تأسيسًا على ما سبق يتضح مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر.

جدول (13)

أراء الشباب حول معاقبة القانون على الجرائم الإلكترونية

النوع / الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	42	21.0	47	23.5	89	22.3
أحياناً	66	33.0	43	21.5	109	27.3
نعم	54	27.0	53	26.5	107	26.8
لا أعرف	38	19.0	57	28.5	95	23.8
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =8.943   درجة الحرية = 3   مستوى المعنوية=.030 دالة

تدل بيانات الجدول السابق على:

أن (27.3%) من الشباب عينة الدراسة موزعة بنسبة (33.0%) للذكور فى مقابل (21.5%) للإناث يعتقدون بأنه أحيانا ما يعاقب القانون على الجرائم الالكترونية، بينما(26.8%) من الشباب عينة الدراسة موزعة بنسبة (27.0%) للذكور فى مقابل (26.5%) للإناث يعتقدون بأن الجرائم الالكترونية يعاقب عليها القانون، فى حين أن (23.8%) من الشباب عينة الدراسة موزعة بنسبة (19.0%) للذكور فى مقابل (28.5%) للإناث لا يعرفون بموقف القانون من الجرائم الإلكترونية، بينما (22.3%) من الشباب عينة الدراسة موزعة بنسبة (21.0%) للذكور فى مقابل (23.5%) للإناث يعتقدون بأن الجرائم الالكترونية لا يعاقب عليها القانون وهذا قد يشير إلى عدم معرفة للجرائم الإلكترونية معرفة كافية ومن ثم إمكانية إرتكابها دون أن يعوا أن هذا يوقعهم تحت طائلة القانون.

تأسيساً على ما سبق يتضح يوجد فروق ذات دلالة إحصائية بين النوع والاعتقاد بمعاقبة القانون على الجرائم الإلكترونية عند 0.05.

جدول رقم (14)
الهدف من ارتكاب الجريمة الإلكترونية

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
الإنتقام	56	28.0	54	27.0	110	27.5	.224	غير دالة
السرقة	78	39.0	53	26.5	131	32.8	2.660	دالة**
الإرهاب	29	14.5	44	22.0	73	18.3	1.939	دالة*
التهديد	30	15.0	27	13.5	57	14.3	.429	غير دالة
التشهير	53	26.5	66	33.0	119	29.8	1.420	غير دالة
الإبتزاز	67	33.5	72	36.0	139	34.8	.524	غير دالة
الحصول على المعلومات	87	43.5	59	29.5	146	36.5	2.904	دالة**
القتل	67	33.5	43	21.5	110	27.5	2.684	دالة**
أخرى	3	1.5	8	4.0	11	2.8	1.527	غير دالة
جملة من سئلوا	**200**		**200**		**400**			

أوضحت بيانات الجدول السابق أن الهدف من ارتكاب الجريمة الإلكترونية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاء الحصول على المعلومات فى مقدمة الأهداف لإرتكاب الجريمة الإلكترونية بنسبة بلغت (36.5%)، موزعة بنسبة (43.5%) للذكور فى مقابل (29.5%) للإناث. بينما جاء فى الترتيب الثانى من أهداف ارتكاب الجريمة الإلكترونية الإبتزاز بنسبة بلغت (34.8%)، موزعة بنسبة (33.5%) للذكور فى مقابل (36.0%) للإناث. بينما جاء فى الترتيب الثالث من أهداف ارتكاب الجريمة الإلكترونية السرقة بنسبة بلغت (32.8%)، موزعة بنسبة (39.0%) للذكور فى مقابل (26.5%) للإناث. بينما جاء فى الترتيب الرابع من أهداف ارتكاب الجريمة الإلكترونية التشهير بنسبة بلغت (29.8%)، موزعة بنسبة (26.5%) للذكور فى مقابل (33.0%) للإناث، بينما جاء فى الترتيب الخامس من أهداف ارتكاب الجريمة الإلكترونية القتل والإنتقام بنسبة بلغت (27.5.%) لكل منهم، بينما جاء فى الترتيب السادس من أهداف ارتكاب الجريمة الإلكترونية الارهاب بنسبة بلغت (18.3%) موزعة بنسبة (14.5%) للذكور فى مقابل (22.0%) للإناث، بينما جاء فى الترتيب السابع من أهداف ارتكاب الجريمة

الإلكترونية التهديد بنسبة بلغت (14.3%)، موزعة بنسبة (15.0%) للذكور فى مقابل (13.5%) للإناث، بينما جاء فى الترتيب الثامن من أهداف ارتكاب الجريمة الإلكترونية أهداف أخرى غير المذكورة بالجدول لم تفصح عنها العينة بنسبة بلغت (2.8%)، موزعة بنسبة (1.5%) للذكور فى مقابل (4.0%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحصائيا بين الذكور والإناث في أرائهم حول الهدف من ارتكاب الجريمة الإلكترونية على النحو الأتى.

- تزداد نسبة الذكور الذين يرون ان الحصول على المعلومات فى مقدمة الأهداف لإرتكاب الجريمة الإلكترونية عن الإناث (43.5%)، (29.5%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة (2.904) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين بمستوى ثقة (99%). وقد يعكس ذلك إلى أن الذكور أكثر وعيا من الإناث فى معرفة أهداف الجريمة الإلكترونية.

- تزداد نسبة الذكور الذين يرون أن السرقة هدف من أهداف إرتكاب الجريمة الإلكترونية عن الإناث بنسبة بلغت (39.0%)، (26.5%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة (2.660) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (99%). وقد يعكس ذلك إلى أن الذكور أكثر وعيا من الإناث فى معرفة أهداف الجريمة الإلكترونية ربما لأنهم الأكثر متابعة لها بالدراما الاجنبية.

- تزداد نسبة الإناث الذين يرون أن الارهاب هدف من أهداف إرتكاب الجريمة الإلكترونية عن الذكوربنسبة بلغت(22.0%)، (14.5%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(1.939) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- تزداد نسبة الذكور الذين يرون أن القتل هدف من أهداف إرتكاب الجريمة الإلكترونية عن الإناث بنسبة (33.0%)، (21.0%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(2.684) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (99%).

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث في أراءهم حول الهدف من ارتكاب الجريمة الإلكترونيةعلى النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الانتقام هدف من أهداف إرتكاب الجريمة الإلكترونية بنسبة (28.0%)، (27.0%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (224.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن التهديد هدف من أهداف إرتكاب الجريمة الإلكترونية بنسبة (15.0%)، (13.5%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (429.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن التشهير هدف من أهداف إرتكاب الجريمة الإلكترونية بنسبة (26.5%)، (33.0%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.420) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الابتزاز هدف من أهداف إرتكاب الجريمة الإلكترونية بنسبة (33.5%)، (36.0%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (524.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن هناك أهدف أخرى لإرتكاب الجريمة الإلكترونية بنسبة (1.5%)، (4.0%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.527) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

جدول رقم (15)

أسباب ارتكاب الجريمة الإلكترونية

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
المنفعة المادية	128	64.0	70	35.0	198	49.5	5.793	دالة***
الشعور بالفراغ	74	37.0	87	43.5	161	40.3	1.324	غير دالة
الفضول	46	23.0	52	26.0	98	24.5	.697	غير دالة
الرغبة فى إثبات الذات	62	31.0	58	29.0	120	30.0	.436	غير دالة
التسلية واللهو	76	38.0	76	38.0	152	38.0	.000	غيردالة
استكشاف عالم الشبكة المعلوماتية	50	25.0	47	23.5	97	24.3	.350	غير دالة
الإثارة والمتعة والتحدى	50	25.0	47	23.5	97	24.3	.350	غير دالة
الإرهاب والتجسس	83	41.5	81	40.5	164	41.0	.203	غير دالة
ارتكاب الجرائم كوسيلة للدعابة	32	16.0	48	24.0	80	20.0	1.997	دالة*
الشعور بالنقص	41	20.5	53	26.5	94	23.5	1.413	غير دالة
الغرور	20	10.0	30	15.0	50	12.5	1.510	غير دالة
مرض نفسى	62	31.0	93	46.5	155	38.8	3.178	دالة***
مرض اجتماعى	36	18.0	41	20.5	77	19.3	.633	غير دالة
أخرى	12	6.0	12	6.0	24	6.0	.000	غير دالة
جملة من سئلوا	**200**		**200**		**400**			

وأوضحت بيانات الجدول السابق أن أسباب ارتكاب الجريمة الإلكترونية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاءت المنفعة المادية فى مقدمة **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت (49.5%)، موزعة بنسبة (64.0%) للذكور فى مقابل (35.0%) للإناث. بينما جاء فى الترتيب الثانى من **أسباب ارتكاب الجريمة الإلكترونية** الارهاب والتجسس بنسبة بلغت (41.0%)، موزعة بنسبة (41.5%) للذكور فى مقابل (40.5%) للإناث. بينما جاء فى الترتيب الثالث من **أسباب ارتكاب الجريمة الإلكترونية الشعور بالفراغ** بنسبة بلغت (40.3%)، موزعة بنسبة (37.0%) للذكور فى مقابل (43.5%) للإناث. بينما جاء فى الترتيب الرابع من

أسباب ارتكاب الجريمة الإلكترونية أنها مرض نفسى بلغت (38.8%)، موزعة بنسبة بلغت (31.0%) للذكور فى مقابل (46.5%) للإناث، بينما جاء فى الترتيب الخامس من **أسباب ارتكاب الجريمة الإلكترونية** أنها التسلية واللهو بنسبة بلغت (38.0.%) موزعة بنسبة بلغت (38.0%) لكل من الذكور والإناث على السواء، بينما جاء فى الترتيب السادس من **أسباب ارتكاب الجريمة الإلكترونية** الرغبة فى اثبات الذات بنسبة بلغت (30.0%) موزعة بنسبة (31.0%) للذكور فى مقابل (29.0%) للإناث، بينما جاء فى الترتيب السابع من **أسباب ارتكاب الجريمة الإلكترونية** الفضول بنسبة بلغت (24.5%)، موزعة بنسبة (23.0%) للذكور فى مقابل (26.0%) للإناث، بينما جاء فى الترتيب الثامن من **أسباب ارتكاب الجريمة الإلكترونية** كل من (استكشاف عالم الشبكة المعلوماتية) و(الإثارة والمتعة والتحدى) بنسبة بلغت (24.3%) لكل منهما على السواء، بينما جاء فى الترتيب التاسع من **أسباب ارتكاب الجريمة الإلكترونية** الشعور بالنقص بنسبة بلغت (23.5%) موزعة بنسبة (20.5%) للذكور فى مقابل (26.5%) للإناث، بينما جاء فى الترتيب العاشر من **أسباب ارتكاب الجريمة الإلكترونية** ارتكاب الجرائم كوسيلة للدعابة بنسبة بلغت (20.0%) موزعة بنسبة (16.0%) للذكور فى مقابل (24.0%) للإناث، بينما جاء فى الترتيب الحادى عشر من **أسباب ارتكاب الجريمة الإلكترونية** أنها مرض اجتماعى بنسبة بلغت (19.3%) موزعة بنسبة (18.0%) للذكور فى مقابل (20.5%) للإناث، بينما جاء فى الترتيب الثانى عشر من **أسباب ارتكاب الجريمة الإلكترونية** الغرور بنسبة بلغت (12.5%) موزعة بنسبة (10.0%) للذكور فى مقابل (15.0%) للإناث، بينما جاء فى الترتيب الثالث عشر من **أسباب ارتكاب الجريمة الإلكترونية** أسباب أخرى غير المذكورة بالجدول لم تفصح عنها العينة بنسبة بلغت (6.0%) موزعة بنسبة (6.0%) للذكور فى مقابل (6.0%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحصائيا بين الذكور والإناث في أسباب ارتكاب الجريمة الإلكترونيةعلى النحو الأتى:

- تزداد نسبة الذكور الذين يرون ان المنعة المادية فى مقدمة الأسباب لإرتكاب الجريمة الإلكترونية عن الإناث (64.0%)، (35.0%) على الترتيب، والفارق دال إحصائيا بلغت قيمة Z المحسوبة (5.793) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين

عند بمستوى ثقة (999%) وقد يرجع ذلك إلى ارتفاع نسبة مشاهدة الذكور للدراما الأجنبية بوجه عام و الدراما التى تقدم جريمة إلكترونية بوحه خاص وذلك وفقا لجول رقم (2)،(8) بالدراسة الميدانية وخاصة ان معظم الجرائم المقدمة عن الجرائم الإلكترونية كان سببها المنفعة المادية وفقا لجول رقم (10) من الدراسة التحليلية.

- تزداد نسبة الإناث الذين يرون ان ارتكاب الجرائم كوسيلة للدعابة أحد أسباب إرتكاب الجريمة الإلكترونية عن الذكور (16.0%)، (24.0%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(1.997) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%) قد تعكس هذه النتائج وعى المراهقيت من الإناث ببعض أسباب الجريمة الإلكترونية أكثر من الذكور فبالفعل قد يرتكب بعض الشباب هذه الجرائم كشكل من اشكال الدعابة نظرا لعدم وعيهم بمدى خطورة هذه الجرائم وأثارها الجسيمة.

- تزداد نسبة الإناث الذين يرون ان المرض النفسى أحد أسباب إرتكاب الجريمة الإلكترونية عن الذكور على الترتيب(31.0%)، (46.5%)، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(3.178) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (99%).

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث في أسباب ارتكاب الجريمة الإلكترونيةعلى النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الانتقام هدف من أهداف إرتكاب الجريمة الإلكترونية بنسبة (28.0%)،(27.0%)على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (224.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الارهاب والتجسس أحد **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت (41.5%)، (40.5%) على الترتيب.

والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (203.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الشعور بالفراغ أحد أسباب ارتكاب الجريمة الإلكترونية بنسبة بلغت(37.0%)، (43.5%) على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.324) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن التسلية واللهوأحد **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت (38.0%) لكل منهم على السواء.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (000.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن **الرغبة فى اثبات الذات** أحد **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت(31.0%)، (29.0%) على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (436.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن **الفضول** أحد **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت((23.0%)، (26.0%) على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (697.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن كل من (استكشاف عالم الشبكة المعلوماتية) و(الإثارة والمتعة والتحدى) أحد **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت بنسبة بلغت ((25.0%)، (23.5%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (350.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

– يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الشعور بالنقص أحد **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت بنسبة بلغت (20.5%)، (26.5%)على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.413) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
– يتقارب نسبة الشباب الذكور والإناث الذين يرون أن المرض الاجتماعى أحد **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت (18.0%)، (20.5%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (633.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

– يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الغرور أحد **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت بنسبة بلغت (10.0%)، (15.0%)على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.510) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

يتقارب نسبة الشباب الذكور والإناث الذين يرون أن أسباب أخرى غير المذكورة بالجدول لم تفصح عنها العينة أحد **أسباب ارتكاب الجريمة الإلكترونية** بنسبة بلغت بنسبة بلغت (6.0%)، (6.0%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (000.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

تأسيسًا على ما سبق تعددت أسباب ارتكاب الجريمة الإلكترونية من وجهة نظر الشباب عينة الدراسة .

جدول رقم (16)

أسباب انتشار الجريمة الإلكترونية فى مصر والدول العربية

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
ضعف القوانين.	117	58.5	104	52.0	221	55.3	1.306	غير دالة
قلة الوازع الدينى	80	40.0	101	50.5	181	45.3	2.107	دالة*
زيادة قاعدة مستخدمى الإنترنت	66	33.0	77	38.5	143	35.8	1.146	غير دالة
انتشار البطالة	87	43.5	111	55.5	198	49.5	2.397	دالة**
الفراغ	87	34.5	93	46.5	180	45.0	.602	غير دالة
الجهل	46	23.0	62	31.0	108	27.0	1.800	غير دالة
الميل للإجرام	43	21.5	50	25.0	93	23.3	.828	غير دالة
القصور فى برامج التوعية	55	27.5	61	30.5	116	29.0	.660	غير دالة
الأمراض النفسية والإجتماعية	56	28.0	76	38.0	132	33.0	2.124	دالة*
أخرى	15	7.5	8	4.0	23	5.8	1.502	غير دالة
جملة من سئلوا	**200**		**200**		**400**			

أوضحت بيانات الجدول السابق أن أسباب انتشار الجريمة الإلكترونية فى مصر والدول العربية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاء ضعف القوانين فى مقدمة أسباب نتشار الجريمة الإلكترونية فى مصر والدول العربيةبنسبة بلغت (55.3%)، موزعة بنسبة (58.5%) للذكور فى مقابل (52.0%) للإناث تشير هذه النتيجة إلى وعى الشباب بأن القوانين المعدة لعقاب مرتكبى الجرائم الإلكترونية غير رادعة لمنعم من ارتكابها. بينما جاء فى الترتيب الثانى انتشار البطالة كأحد أسباب نتشار الجريمة الإلكترونية فى مصر بنسبة بلغت (49.5%)، موزعة بنسبة (43.5%) للذكور فى مقابل (55.5%) للإناث وقد يرجع ذلك إلى وعى الشباب بأن البطالة تخلق حالة من الفراغ تجعل الكثير من الشباب يخرج عن المسار الصحيح والطريق السليم.. بينما جاء فى الترتيب الثالث قلة الوازع الدينى

كأحد أسباب نتشار الجريمة الإلكترونية فى مصر بنسبة بلغت (45.3%)، موزعة بنسبة (40.0%) للذكور فى مقابل (50.5%) للإناث قد تشير هذه النتيجة إلى وعى الشباب بأن قلة الوازع الدينى تجعل الانسان يفعل ما يشاء دون الخوف فى عقاب الله.بينما جاء فى الترتيب الرابع الفراغ كأحد أسباب نتشار الجريمة الإلكترونية فى مصر بنسبة بلغت (45.0%)، موزعة بنسبة (43.5%) للذكور فى مقابل (46.5%) للإناث.بينما جاء فى الترتيب الخامس زيادة قاعدة مستخدمى الانترنت كأحد أسباب نتشار الجريمة الإلكترونية فى مصر بنسبة بلغت (35.8%)، موزعة بنسبة (33.0%) للذكور فى مقابل (38.5%) للإناث. بينما جاء فى الترتيب السادس الأمراض النفسية والاجتماعية كأحد أسباب نتشار الجريمة الإلكترونية فى مصر بنسبة بلغت (33.0%)، موزعة بنسبة (28.0%) للذكور فى مقابل (38.0%) للإناث. بينما جاء فى الترتيب السابع القصور فى برامج التوعية كأحد أسباب نتشار الجريمة الإلكترونية فى مصر بنسبة بلغت (29.0%)، موزعة بنسبة (27.5%) للذكور فى مقابل (30.5%) للإناث. بينما جاء فى الترتيب الثامن الجهل كأحد أسباب نتشار الجريمة الإلكترونية فى مصر بنسبة بلغت (27.0%)، موزعة بنسبة (23.0%) للذكور فى مقابل (31.0%) للإناث. بينما جاء فى الترتيب التاسع الميل للإجرام كأحد أسباب نتشار الجريمة الإلكترونية فى مصر بنسبة بلغت (23.3%)، موزعة بنسبة (21.5%) للذكور فى مقابل (25.0%) للإناث.. بينما جاء فى الترتيب العاشر أن هناك أسباب اخرى غير المذكورة بالجدول لم تفصح عنها العينة كأحد أسباب انتشار الجريمة الإلكترونية فى مصر بنسبة بلغت (5.8%)، موزعة بنسبة (7.5%) للذكور فى مقابل (4.0%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحصائيا بين الذكور والإنــاث في أسباب ارتكاب الجريمة الإلكترونيةعلى النحو الأتى:

- تزداد نسبة الإناث الذين يرون أن قلة الوازع الدينى أحد **أسباب نتشار الجريمة الإلكترونية فى مصر** عن الذكور (40.0%)، (50.5%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(2.107) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- تزداد نسبة الإناث الذين يرون أن انتشار البطالة أحد **أسباب نتشار الجريمة الإلكترونية فى مصر** عن الذكور (43.5%)، (55.5%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(2.397) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (99%).

- تزداد نسبة الإناث الذين يرون أن الأمراض النفسية والاجتماعية أحد **أسباب نتشار الجريمة الإلكترونية فى مصر** (28.0%)، (38.0%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(2.124) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الـذكور والإناث في أسباب ارتكاب الجريمة الإلكترونيةعلى النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن ضعف أحد **أسباب انتشار الجريمة الإلكترونية فى مصر** بنسبة (58.5%)، (52.0%)على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.306) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الفراغ أحد **أسباب انتشار الجريمة الإلكترونية فى مصر** بنسبة (43.5%)، (46.5%)على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (602.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن زيادة قاعدة مستخدمى الانترنت أحد **أسباب انتشار الجريمة الإلكترونية فى مصر** بنسبة (33.0%)، (38.5%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.146) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن القصور فى برامج التوعية أحد **أسباب انتشار الجريمة الإلكترونية فى مصر** بنسبة (27.5%)، (30.5%)على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (660.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الجهل أحد **أسباب انتشار الجريمة الإلكترونية فى مصر** بنسبة (23.0%)، (31.0%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.800) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن الميل للإجرام أحد **أسباب انتشار الجريمة الإلكترونية فى مصر** بنسبة (21.5%)،(25.0%).

- على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (828.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون أن هناك أسباب أخرى غير المذكورة بالجدول لم تفصح عنها العينة أحد **أسباب انتشار الجريمة الإلكترونية فى مصر** بنسبة (7.5%)، (4.0%)على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (828.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

تأسيسًا على ما سبق أن هناك أسباب لانتشار الجريمة الإلكترونية فى مصر

جدول (17)

اعتقاد الشباب وجود أشكال متعددة للجريمة الإلكترونية

النوع / الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	6	3.0	1	.5	7	1.8
أحياناً	14	7.0	18	9.0	32	8.0
نعم	180	90.0	181	90.3	361	90.3
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =**4.074** درجة الحرية = **2** مستوى المعنوية=**130.** غير دالة

تدل بيانات الجدول السابق على:

أن (90.3%) من الشباب عينة الدراسة موزعة بنسبة (90.0%) للذكور فى مقابل (90.3%) للإناث يعتقدون فى وجود أشكال متعددة للجرائم الإلكترونية مما قد يعكس معرفة الشباب بالجريمة الإلكترونية وأشكالها المختلفة وقد يرجع ذلك إلى متابعة الدراما الأجنبية وربما يرجع لأسباب أخرى،فى حين أن (8.0%) من الشباب عينة الدراسة موزعة بنسبة (7.0%) للذكور فى مقابل (9.0%) للإناث يعتقدون بأنه أحيانا يوجد أشكال متعددة للجرائم الإلكترونية،بينما(1.8%) من الشباب عينة الدراسة موزعة بنسبة (3.0%) للذكور فى مقابل (5.%) للإناث يعتقدون فى عدم وجود أشكال متعددة للجرائم الإلكترونية.

تأسيساًعلى ما سبق يتضح بأنه لا يوجد فروق ذات دلالة إحصائية بين النوع و الاعتقاد فى وجود أشكال متعددة للجرائم الإلكترونية.

جدول (18)
أشكال الجريمة الإلكترونية

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
القرصنة	147	75.8	120	60.3	267	67.9	3.281	دالة***
بيع المخدرات عبر الإنترنت	49	25.3	58	29.1	107	27.2	.865	غير دالة
سرقة بعض الحسابات البنكية	116	59.8	114	57.3	230	58.5	.504	غير دالة
الإرهاب الإلكترونى	43	22.2	55	27.6	98	24.9	1.252	غير دالة
تدمير الملفات	83	42.8	81	40.7	164	41.7	.418	غير دالة
لتجسس	102	52.6	105	52.3	207	52.7	.037	غير دالة
التعرض للمواقع الأباحية	81	41.8	102	51.3	183	46.6	1.886	دالة*
التشهير	37	19.1	63	31.7	100	25.4	2.860	دالة**
السب والقذف	40	20.6	56	28.1	96	24.4	1.733	غير دالة
غسيل الأموال	41	21.1	59	29.6	100	25.4	1.935	دالة*
الاحتيال	51	26.3	54	27.1	105	26.7	.189	غير دالة
المقامرة	29	14.9	24	12.1	53	13.5	.837	غير دالة
أخرى	7	3.6	10	5.0	17	4.3	.689	غير دالة
جملة من سئلوا	**194**		**199**		**393**			

أوضحت بيانات الجدول السابق أشكال الجريمة الإلكترونية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاءت **القرصنة** فى مقدمة **أشكال الجريمة الإلكترونية** بنسبة بلغت (67.9%)، موزعة بنسبة (75.8%) للذكور فى مقابل (60.3%) للإناث، بينما جاء فى **الترتيب الثانى سرقة بعض الحسابات البنكية** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(58.5%) موزعة بنسبة (59.8%) للذكور فى مقابل (57.3%) للإناث بينما جاء فى **الترتيب الثالث التجسس** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(52.7%) موزعة بنسبة (52.6%) للذكور فى مقابل (52.8%) للإناث. بينما جاء فى **الترتيب الرابع التعرض للمواقع الاباحية** كأحد أشكال الجرائم الإلكترونيةبنسبة

بلغت(46.6%) موزعة بنسبة (41.8%) للذكور فى مقابل (51.3%) للإناث. بينما جاء فى **الترتيب الخامس تدمير الملفات** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(41.7%) موزعة بنسبة (42.4%) للذكور فى مقابل (40.7%) للإناث. بينما جاء فى **الترتيب السادس بيع المخدرات عبر الانترنت** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(27.2%) موزعة بنسبة (25.3%) للذكور فى مقابل (29.1%) للإناث. بينما جاء فى **الترتيب السابع الاحتيال** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(26.7%) موزعة بنسبة (26.3%) للذكور فى مقابل (27.1%) للإناث.. بينما جاء فى **الترتيب الثامن كل من التشهير وغسيل الأموال** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(25.4%). بينما جاء فى **الترتيب التاسع الإرهاب الإلكترونى** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(24.9%) موزعة بنسبة (22.2%) للذكور فى مقابل (27.6%) للإناث.

بينما جاء فى **الترتيب العاشر السب والقذف** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(24.4%) موزعة بنسبة (20.6%) للذكور فى مقابل (24.4%) للإناث. بينما جاء فى **الترتيب الحادى عشر المقامرة** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(13.5%) موزعة بنسبة (14.9%) للذكور فى مقابل (12.1%) للإناث. بينما جاء فى **الترتيب الثانى عشر أشكال أخرى غير المذكورة بالجدول لم تفصح عنها العينة** كأحد أشكال الجرائم الإلكترونية بنسبة بلغت(4.3%) موزعة بنسبة (3.6%) للذكور فى مقابل (5.0%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحصائيا بين الذكور والإناث في أضرار الجريمة الإلكترونية على النحو الأتى.

- تزداد نسبة الذكور الذين يرون **أن القرصنة** فى مقدمة **أشكال الجريمة الإلكترونية عن الاناث** بنسبة (75.8%)، (60.3%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(3.281) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (999%).

- تزداد نسبة الإناث الذين يرون **أن التعرض للمواقع الاباحية** أحد **أشكال الجريمة الإلكترونية عن الذكور** بنسبة (51.3%)، (41.8%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(1.886) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- تزداد نسبة الإناث الذين يرون **أن التشهير** أحد **أشكال الجريمة الإلكترونية عن الذكور** بنسبة(31.7%)، (19.1%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة (2.860) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (99%).

- تزداد نسبة الإناث الذين يرون **أن غسيل الأموال** أحد **أشكال الجريمة الإلكترونية عن الذكور** بنسبة(29.6%)، (21.1%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.935) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث حول أضرار الجريمة الإلكترونية على النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن سرقة بعض الحسابات البنكية** أحد أشكال الجرائم الإلكترونية بنسبة (59.8%)، (57.3%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (.504) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن التجسس** أحد أشكال الجرائم الإلكترونية (52.6%)، (52.8%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (.037) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن تدمير الملفات** أحد أشكال الجرائم الإلكترونية بنسبة (42.4%)، (40.7%) على الترتيب. والفارق غير دال

إحصائيا حيث بلغت قيمة Z المحسوبة (418.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن بيع المخدرات عبر الانترنت** كأحد أشكال الجرائم الإلكترونية (25.3%)، (29.1%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (865.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن الاحتيال**أحد أشكال الجرائم بنسبة (26.3%)، (27.1%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (189.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن االارهاب الالكترونى** أحد أشكال الجرائم الإلكترونية بنسبة (22.2%)، (27.6%) على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.252.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن السب والقذف** أحد أشكال الجرائم الإلكترونية بنسبة (20.6%)، (24.4%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.733) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن المقامرة** أحد أشكال الجرائم الإلكترونية بنسبة (14.9%)، (12.1%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (837.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن أشكال أخرى غير المذكورة بالجدول لم تفصح عنها العينة** أحد أشكال الجرائم الإلكترونية بنسبة (3.6%)، (5.0%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (689.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

جدول رقم (19)

سمات مرتكب الجريمة الإلكترونية

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
بالذكاء	117	58.5	75	37.5	192	48.0	4.198	دالة***
الاجرام	61	30.5	89	44.5	150	37.5	2.888	دالة**
ملم بالتقنيات الحديثة	105	52.5	87	43.5	192	48.0	1.799	غير دالة
العنف	18	9.0	57	28.5	75	18.8	4.990	دالة***
الهدوء	24	12.0	16	8.0	40	10.0	1.332	غير دالة
المراوغة	61	30.5	43	21.5	104	26.0	2.049	دالة*
الإنطواء	44	22.0	53	26.5	97	24.3	1.049	غير دالة
الخبرة والمهارة	77	38.5	50	25.0	127	31.8	2.896	دالة**
الميل للتقليد	32	16.0	36	18.0	68	17.0	.532	غير دالة
التخصص فى ارتكاب الجريمة الالكترونية	48	24.0	52	26.0	100	25.0	.461	غير دالة
الاحتراف فى ارتكاب الجريمة الالكترونية	66	33.0	82	41.0	148	37.0	1.655	غير دالة
السلبية	60	30.0	100	50.0	160	40.0	4.077	دالة***
الإيجابية	7	3.5	10	5.0	17	4.3	.743	غير دالة
لا أعرف	2	1.0	8	4.0	10	2.5	1.919	دالة*
أخرى	6	3.0	11	5.5	17	4.3	1.238	غير دالة
جملة من سئلوا	**200**		**200**		**400**			

كما أوضحت بيانات الجدول السابق سمات مرتكب الجريمة الإلكترونية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاءت كل من الذكاء والإلمام بالتكنولوجيا الحديثة فى مقدمة **سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (48.0%) وقد يشير ذلك إلى إلمام العينة بسمات مرتكبى الجريمة الإلكترونية. بينما جاء فى **الترتيب الثانى الاجرام كسمة من سمات**

مرتكبى الجريمة الإلكترونية بنسبة بلغت (37.5%)، موزعة بنسبة (30.5%) للذكور فى مقابل (44.5%) للإناث ، بينما جاء فى **الترتيب الثالث السلبية كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (40.0%)، موزعة بنسبة (30.0%) للذكور فى مقابل (50.0%) للإناث. بينما جاء فى **الترتيب الرابع الخبرة والمهارة كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (31.8%)، موزعة بنسبة (38.5%) للذكور فى مقابل (25.0%) للإناث. بينما جاء فى **الترتيب الخامس الاجرام كسمة من سمات فى ارتكاب الجريمة الالكترونية** بنسبة بلغت (37.5%)، موزعة بنسبة (30.5%) للذكور فى مقابل (44.5%) للإناث ، بينما جاء فى **الترتيب السادس الاحتراف فى ارتكاب الجريمة الالكترونية كسمة من سمات مرتكب الجريمة الالكترونية** بنسبة بلغت (37.0%)، موزعة بنسبة (33.0%) للذكور فى مقابل (41.0%) للإناث، بينما جاء فى **الترتيب السابع الخبرة والمهارة كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (31.8%)، موزعة بنسبة (38.5%) للذكور فى مقابل (25.0%) للإناث، بينما جاء فى **الترتيب الثامن الخبرة والمهارة كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (31.8%)، موزعة بنسبة (38.5%) للذكور فى مقابل (25.0%) للإناث. بينما جاء فى **الترتيب التاسع المراوغة كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (26.0%)، موزعة بنسبة (30.5%) للذكور فى مقابل (21.5%) للإناث ،بينما جاء فى **الترتيب العاشر التخصص فى ارتكاب الجريمة الالكترونية كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (25.0%)، موزعة بنسبة (24.0%) للذكور فى مقابل (26.0%) للإناث،بينما جاء فى **الترتيب الحادى عشر الانطواء كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (24.3%)، موزعة بنسبة (22.0%) للذكور فى مقابل (26.5%) للإناث. بينما جاء فى **الترتيب الثانى عشر العنف كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (18.8%)، موزعة بنسبة (9.0%) للذكور فى مقابل (28.5%) للإناث ، بينما جاء فى **الترتيب الثالث عشر الميل للتقليد كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (17.0%)، موزعة بنسبة (16.0%) للذكور فى مقابل (17.0%) للإناث، بينما جاء فى **الترتيب الرابع عشر الهدوء كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (10.0%)، موزعة بنسبة

(12.0%) للذكور فى مقابل (8.0%) للإناث. بينما جاء فى **الترتيب الخامس عشر كل من الإيجابية وأسباب أخرى كسمة من سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (4.3%). بينما جاء فى **الترتيب السادس عشر أن الشباب لا يعرفون سمات مرتكبى الجريمة الإلكترونية** بنسبة بلغت (2.5%)، موزعة بنسبة (1.0%) للذكور فى مقابل (4.0%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحائيا بين الذكور والإناث في سمات مرتكبى الجريمة الإلكترونية على النحو الأتى.

- تزداد نسبة الذكور الذين يرون **أن الذكاء سمة من سمات مرتكبى الجريمة الألكترونية عن الاناث** بنسبة (58.5%)، (37.5%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(4.198) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (999%).
- تزداد نسبة الذكور الذين يرون **أن المراوغة سمة من سمات مرتكبى الجريمة الألكترونية عن الاناث** بنسبة (30.5%)، (21.5%)على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(2.049) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- تزداد نسبة الذكور الذين يرون **أن الخبرة والمهارة سمة من سمات مرتكبى الجريمة الألكترونية عن الاناث** بنسبة (38.5%)، (25.0%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(2.896) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (99%).
- تزداد نسبة الاناث الذين يرون **أن الاجرام سمة من سمات مرتكبى الجريمة الألكترونية عن الذكور** بنسبة (44.5%)، (30.5%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(2.888) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (99%).

- تزداد نسبة الاناث الذين يرون **أن العنف سمة من سمات مرتكبى الجريمة الألكترونية عن الذكور** بنسبة (28.5%)، (9.0%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(4.990) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (999%).

- تزداد نسبة الاناث الذين يرون **أن السلبية سمة من سمات مرتكبى الجريمة الألكترونية عن الذكور** بنسبة (50.0%)، (30.0%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(4.077) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (999%).

- تزداد نسبة الاناث الذين لا يعرفون **سمات مرتكبى الجريمة الألكترونية عن الذكور** بنسبة (50.0%)، (30.0%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة(1.919) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث حول سمات مرتكبى الجريمة الإلكترونية على النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن الالمام بالتقنيات الحديثة سمة من سمات مرتكبى الجريمة الألكترونية** بنسبة (52.5%)، (43.5%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.799) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن الهدوء سمة من سمات مرتكبى الجريمة الألكترونية** بنسبة (12.0%)، (8.0%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.332) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن الانطواء سمة من سمات مرتكبى الجريمة الألكترونية** بنسبة (22.0%)، (26.5%) على الترتيب.

والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.049) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

– يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن الميل للتقليد سمة من سمات مرتكبى الجريمة الألكترونية** بنسبة (16.0%)، (18.0%) على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.049) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

– يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن التخصص فى ارتكاب الجريمة الالكترونية سمة من سمات مرتكبى الجريمة الألكترونية** بنسبة (24.0%)، (26.0%) على الترتيب. والفارق غير دال إحصائيا بلغت قيمة Z المحسوبة (461.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

– يتقارب نسبة الشباب الذكور والإناث الذين يرون **الاحتراف فى ارتكاب الجريمة الالكترونية سمة من سمات مرتكبى الجريمة الألكترونية** بنسبة (33.0%)، (41.0%) على الترتيب. والفارق غير دال إحصائيا بلغت قيمة Z المحسوبة (1.655) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

– يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن الايجابية سمة من سمات مرتكبى الجريمة الألكترونية** بنسبة (3.5%)، (5.0%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (743.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

– يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن اسمات أخرى من سمات مرتكبى الجريمة الألكترونية غير الموجودة بالجدول** بنسبة (05%)، (5.5%) على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.238) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

تأسيساً على ماسبق يتضح وعى الشباب بسمات مرتكبى الجرائم الإلكترونية.

جدول (20)

أراء الشباب حول انتماء مرتكبى الجرائم الإلكترونية لطبقة اجتماعية معينة

النوع / الاعتقاد	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	91	45.5	84	42.0	175	43.8
أحياناً	40	20.0	48	24.0	88	22.0
نعم	69	34.5	68	34.0	137	34.3
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =1.015 درجة الحرية = 2 مستوى المعنوية=602. غير دالة

تدل بيانات الجدول السابق على:

أن (43.8%) من الشباب عينة الدراسة موزعة بنسبة (45.5%) للذكور فى مقابل (42.0%) للإناث يعتقدون أن مرتكبى الجرائم الإلكترونية لا ينتمون إلى طبقة اجتماعية معينة وقد يعكس ذلك وعى الشباب بمدى الاختلاف بين الجريمة الإلكترونية والجريمة التقليدية فارتكاب الجريمة الإلكترونية ليس بالضرورة يكون الهدف منها الكسب المادى أو الإنتقام، بينما (34.3%) من الشباب عينة الدراسة موزعة بنسبة (34.5%) للذكور فى مقابل (34.0%) للإناث يعتقدون أن مرتكبى الجرائم الإلكترونية ينتمون إلى طبقة اجتماعية معينة وقد يرجع ذلك إلى اعتقاد بعض الشباب عينة الدراسة أن الجريمة الإلكترونية يكون أهم أسبابها الكسب المادى، بينما أن (22.0%) من الشباب عينة الدراسة موزعة بنسبة (20.0%) للذكور فى مقابل (24.0%) للإناث يعتقدون أن مرتكبى الجرائم الإلكترونية أحيانا ما ينتمون إلى طبقة اجتماعية معينة.

تأسيساً على ما سبق يتضح بأنه لا يوجد فروق ذات دلالة إحصائية بين النوع والاعتقاد فى انتماء مرتكبى الجرائم الإلكترونية لطبقة اجتماعية معينة

جدول (21)

أراء الشباب فى الطبقات الاجتماعية التى ينتمى إليها مرتكب الجرائم الإلكترونية

النوع / الاعتقاد	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لمستوى اقتصادي اجتماعي مرتفع	29	26.6	27	23.3	56	24.9
مستوى اقتصادي اجتماعي متوسط	24	22.0	18	15.5	42	18.7
مستوى اقتصادي اجتماعي منخفض	18	16.5	19	16.4	37	16.4
لا أعرف	38	34.9	52	44.8	90	40.0
الاجمالى	**109**	**100**	**116**	**100**	**225**	**100**

قيمة كا^2 =2.918 **درجة الحرية = 3** **مستوى المعنوية=404. غير دالة**

تدل بيانات الجدول السابق على:

أن (40.0%) من الشباب عينة الدراسة موزعة بنسبة (34.9%) للذكور فى مقابل (44.8%) للإناث لا يعرفون اى طبقة اجتماعية ينتمى إليها مرتكبى الجرائم الإلكترونية، **بينما** (24.9%) من الشباب عينة الدراسة موزعة بنسبة (26.6%) للذكور فى مقابل (23.3%) للإناث يرون ان مرتكبى الجريمة الإلكترونية ينتمون إلى **المستوى الاقتصادي الاجتماعي المرتفع، فى حين أن**(18.7%) من الشباب عينة الدراسة موزعة بنسبة (22.0%) للذكور فى مقابل (15.5%) للإناث يرون ان مرتكبى الجريمة الإلكترونية ينتمون إلى **المستوى الاقتصادي الاجتماعي المتوسط، بينما أعرب** (16.4%) من الشباب عينة الدراسة موزعة بنسبة (16.5%) للذكور فى مقابل (16.4%) للإناث يرون ان مرتكبى الجريمة الإلكترونية ينتمون إلى **المستوى الاقتصادي الاجتماعي المنخفض وقد تعكس هذه النتيجة اعتقاد الشباب أن الدافع دائما وراء الجريمة غالبا مايكون الكسب المادى.**

تأسيساً على ما سبق يتضح بأنه لا يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب عينة الدراسة حول الطبقة الإجتماعية التى ينتمى إليها مرتكب الجريمة الإلكترونية.

جدول (22)
اعتقاد الشباب حول نوع مرتكبى الجريمة الإلكترونية

النوع الاعتقاد	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
الذكور	125	62.5	124	62.0	249	62.3
الإناث	6	3.0	5	2.5	11	2.8
الإثنين معا	19	9.5	30	15.0	49	12.3
لا أعرف	50	25.0	41	20.5	91	22.8
الاجمالى	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =3.454 درجة الحرية = 3 مستوى المعنوية=327. غير دالة

تدل بيانات الجدول السابق على:

(62.3%) من الشباب عينة الدراسة موزعة بنسبة (62.5%) للذكور فى مقابل (62.0%) للإناث يعتقدون أن مرتكبى الجرائم الإلكترونية دائما ما يكونوا من الذكور. **بينما** (22.8%) من الشباب عينة الدراسة موزعة بنسبة (25.0%) للذكور فى مقابل (20.5%) للإناث لا يعرفون إلى أى نوع ينتمى مرتكبى الجريمة الإلكترونية، **فى حين أن** (12.3%) من الشباب عينة الدراسة موزعة بنسبة (9.5%) للذكور فى مقابل (15.0%) للإناث أن مرتكبى الجرائم الإلكترونية من الذكور والإناث معا، **فى الوقت الذى يرى فيه** (2.8%) من الشباب عينة الدراسة موزعة بنسبة (3.0%) للذكور فى مقابل (2.5%) للإناث يرون أن مرتكبى الجرائم الإلكترونية من الإناث وهى نسبة قليلة جدا.

تأسيساً على ما سبق يتضح بأنه لا يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب عينة الدراسة حول نوع مرتكب الجريمة الإلكترونية.

جدول رقم (23)

أكثر الفئات العمرية ارتكابا للجريمة الإلكترونية

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
الأطفال	4	2.0	9	4.5	13	3.3	1.408	غير دالة
المراهقون	142	71.0	126	63.0	268	67.0	1.699	غير دالة
الشباب	154	77.0	168	84.0	322	80.5	1.765	غير دالة
كبار السن	11	505	16	8.0	27	6.8	.995	غير دالة
جملة من سئلوا	**200**		**200**		**400**			

أوضحت بيانات الجدول السابق أكثر الفئات العمرية ارتكابا للجريمة الإلكترونية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاء فى مقدمة **الفئات العمرية ارتكابا للجريمة الإلكترونية الشباب** بنسبة بلغت (80.5%)، موزعة بنسبة (77.0%) للذكور فى مقابل (84.0%) للإناث. بينما جاء فى الترتيب الثانى من**الفئات العمرية المرتكبة للجريمة الإلكترونية المراهقون** بنسبة بلغت (67.0%)، موزعة بنسبة (71.0%) للذكور فى مقابل (63.0%) للإناث، بينما جاء فى الترتيب الثالث من**الفئات العمرية المرتكبة للجريمة الإلكترونية كبار السن** بنسبة بلغت (6.8%)، موزعة بنسبة (5.5%) للذكور فى مقابل (8.0%) للإناث، بينما جاء فى الترتيب الرابع من**الفئات العمرية المرتكبة للجريمة الإلكترونية الأطفال** بنسبة بلغت (3.3%)، موزعة بنسبة (2.0%) للذكور فى مقابل (4.5%) للإناث.

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث حول أكثر الفئات العمرية ارتكابا للجريمة الإلكترونية على النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن أكثر الفئات العمرية ارتكابا للجريمة الإلكترونية الشباب** بنسبة بلغت (77.0%)، (84.0%)على الترتيب.

والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.765) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن أكثر الفئات العمرية ارتكابا للجريمة الإلكترونية المراهقون** بنسبة بلغت (71.0%)، (63.0%) للإناث على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.699) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن أكثر الفئات العمرية ارتكابا للجريمة الإلكترونية كبار السن** (5.5%)، (8.0%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (995.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن أكثر الفئات العمرية ارتكابا للجريمة الإلكترونية الأطفال** (2.0%)، (4.5%) للإناث. على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.408) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

تأسيساً على ما سبق يتضح أن اكثر الفئات إرتكابا للجريمة الإلكترونية من الشباب.

جدول (24)

أراء الشباب حول أضرار الجريمة الإلكترونية

النوع / الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
أحياناً	26	13.0	23	11.5	49	12.3
نعم	174	87.0	177	88.5	351	87.8
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =209.   درجة الحرية = 1   مستوى المعنوية=647. غير دالة

تدل بيانات الجدول السابق على:

أن (87.8%) من الشباب عينة الدراسة موزعة بنسبة (87.0%) للذكور فى مقابل (88.5%) للإناث يرون أن الجرائم الإلكترونية لها أضرار، **بينما** (12.3%) من الشباب عينة الدراسة موزعة بنسبة (13.0%) للذكور فى مقابل (11.5%) للإناث يرون أن الجرائم الإلكترونية أحيانا مايكون لها أضرار مجمل نتائج الجدول تشير إلى وعى الشباب بخطورة الجريمة الإلكترونية وما قد تتسبب فيه من أضرار.

تأسيساً على ما سبق يتضح بأنه لا يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب عينة الدراسة حول أضرار الجريمة الإلكترونية.

جدول رقم (25)
أضرار الجريمة الإلكترونية من وجهة نظرك

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
أضرار سلبية على الإقتصاد	81	40.5	66	33.0	147	36.8	1.554	غير دالة
أضرار إجتماعية	92	46.0	85	42.5	177	44.3	.704	غير دالة
أضرار علمية وتكنولجية	48	24.0	31	15.5	79	19.8	2.132	دالة*
تسهيل الإتصال بين الجماعات الإرهابية	57	28.5	59	29.5	116	29.0	.220	غير دالة
تسهيل سرقة أموال المودعين بالبنوك	72	36.0	79	39.5	151	37.8	.721	غير دالة
إختراق اجهزة الأخرين وإنتهاك خصوصيتهم	88	44.0	92	46.0	180	45.0	.402	غير دالة
إتلاف بعض المعلومات الهامة	76	38.0	68	34.0	144	36.0	.832	غير دالة
أخرى	14	7.0	16	8.0	30	7.5	379	غير دالة
جملة من سئلوا	**200**		**200**		**400**			

أوضحت بيانات الجدول السابق أضرار الجريمة الإلكترونية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاء إختراق اجهزة الأخرين وإنتهاك خصوصيتهم فى مقدمة **أضرار الجريمة الإلكترونية** بنسبة بلغت (45.0%)، موزعة بنسبة (44.0%) للذكور فى مقابل (46.0%) للإناث.بينما جاءت **الأضرار الاجتماعية فى الترتيب الثانى** كأحد أضرار الجريمة الإلكترونية بنسبة بلغت (44.3%)، موزعة بنسبة (46.0%) للذكور فى مقابل (42.5%) للإناث. بينما جاء **تسهيل سرقة أموال المودعين بالبنوك فى الترتيب الثالث** كأحد أضرار الجريمة الإلكترونية بنسبة بلغت (37.8%)، موزعة بنسبة (36.0%) للذكور فى مقابل (39.5%) للإناث. بينما جاءت **الأضرار السلبية على الاقتصاد فى الترتيب الرابع** كأحد أضرار الجريمة الإلكترونية بنسبة بلغت (36.8%)، موزعة بنسبة (40.5%) للذكور فى مقابل (33.0%) للإناث. بينما جاء **اتلاف بعض المعلومات الهامة فى الترتيب الخامس** كأحد أضرار الجريمة الإلكترونية بنسبة بلغت (36.0%)، موزعة بنسبة (38.0%) للذكور فى مقابل

(34.0%) للإناث. بينما جاء **تسهيل الاتصال بين الجماعات الارهابية فى الترتيب السادس** كأحد أضرار الجريمة الإلكترونية بنسبة بلغت (29.0%)، موزعة بنسبة (28.5%) للذكور فى مقابل (29.5%) للإناث. جاءت **الأضرار العلمية والتكنولوجية فى الترتيب السابع** كأحد أضرار الجريمة الإلكترونية بنسبة بلغت (19.8%)، موزعة بنسبة (24.0%) للذكور فى مقابل (15.5%) للإناث. جاءت **أضرار أخرى غير المذكورة بالجدول لم تفصح عنها العينة فى الترتيب الثامن** كأحد أضرار الجريمة الإلكترونية بنسبة بلغت (7.5%)، موزعة بنسبة (7.0%) للذكور فى مقابل (8.0%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحصائيا بين الذكور والإناث في أضرار الجريمة الإلكترونية على النحو الأتى:

- تزداد نسبة الذكور الذين يرون **أن الأضرار العلمية والتكنولوجية** كأحد أضرار الجريمة الإلكترونية عن الاناث بنسبة (24.0%)، (15.5%) على الترتيب، والفارق دال إحصائيا حيث بلغت قيمة Z المحسوبة (2.132) وهى أعلى من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث حول أضرار الجريمة الإلكترونية على النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن إختراق اجهزة الأخرين وإنتهاك خصوصيتهم** فى مقدمة **أضرار الجريمة الإلكترونية** بنسبة (44.0%)، (46.0%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (402.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن الأضرار الاجتماعية** أحد أضرار الجريمة الإلكترونية بنسبة (46.0%)، (42.5%) على الترتيب.والفارق غير

دال إحصائيا حيث بلغت قيمة Z المحسوبة (.704) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن تسهيل سرقة أموال المودعين بالبنوك أحد** أضرار الجريمة الإلكترونية (36.0%)، (39.5%) للإناث على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (.721) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن الأضرار السلبية على الاقتصاد** أحد أضرار الجريمة الإلكترونية بنسبة (40.5%)، (33.0%) للإناث على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.554) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن اتلاف بعض المعلومات الهامة** أحد أضرار الجريمة الإلكترونية بنسبة (38.0%)، (34.0%) للإناث على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (.832) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن تسهيل الاتصال بين الجماعات الارهابية** أحد أضرار الجريمة الإلكترونية بنسبة (28.5%)، (29.5%) على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (.220) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن**هناك **أضرار أخرى غير المذكورة بالجدول لم تفصح عنها العينة** أحد أضرار الجريمة الإلكترونية بنسبة (7.0%)، (8.0%) للإناث على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (.379) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

جدول (26)

أراء الشباب حول أضرار الجريمة الإلكترونية جسيمة كالجريمة التقليدية

النوع الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	44	22.0	31	15.5	75	18.8
أحياناً	66	33.0	73	36.5	139	34.8
نعم	90	45.0	96	48.0	186	46.5
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =2.799 درجة الحرية = 2 مستوى المعنوية=247. غيردالة

تدل بيانات الجدول السابق على:

أن (46.5%) من الشباب عينة الدراسة موزعة بنسبة (45.0%) للذكور فى مقابل (48.0%) للإناث يرون أن الجريمة الإلكترونية لها أضرار جسيمة كالجريمة التقليدية وقد تشير هذه النتيجة إلى وعى الشباب بحجم الخطر الناتج عن الجريمة الإلكترونية حتى ولو كانت جريمة ترتكب عبر زر الكمبيوتر، بينما (34.8%) من الشباب عينة الدراسة موزعة بنسبة (33.0%) للذكور فى مقابل (36.0%) للإناث يرون أن الجريمة الإلكترونية لها أضرار جسيمة كالجريمة التقليدية، بينما (18.8%) من الشباب عينة الدراسة موزعة بنسبة (22.0%) للذكور فى مقابل (15.5%) للإناث يرون أن الجريمة الإلكترونية ليس لها أضرار جسيمة كالجريمة التقليدية وقد تشير هذه النتيجة إلى أحد أمرين إما عدم إدراك خطورة الجريمة الإلكترونية أو التهاون فى الأضرار الناتجة عنها والنظر إليها على أنها أمر عادى.

تأسيساً على ما سبق يتضح أنه لا يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب عينة الدراسة حول أضرار الجريمة الإلكترونية جسيمة كالجريمة التقليدية.

جدول (27)

أراء الشباب حول أكثر الفئات تعرضا لمخاطر الجريمة الإلكترونية

النوع / الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
الأفراد ذات المستوى الاجتماعى الاقتصادى المرتفع	102	51.0	75	37.5	177	44.3
الأفراد ذات المستوى الاجتماعى الاقتصادى متوسط	35	17.5	27	13.5	62	15.5
الأفراد ذات المستوى الاجتماعى الاقتصادى منخفض	19	9.5	29	14.5	48	12.0
لا أعرف	44	22.0	69	34.5	113	28.3
حملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =12.765   درجة الحرية = 3   مستوى المعنوية=005. دالة

تدل بيانات الجدول السابق على:

أن(44.3%) من الشباب عينة الدراسة موزعة بنسبة (51.0%) للذكور فى مقابل (37.5%) للإناث يرون أن أكثر الفئات تعرضا لمخاطر الجريمة الإلكترونية الأفراد ذات المستوى الاجتماعى الاقتصادى المرتفع وقد يرجع ذلك إلى اعتقاد الشباب أن الجرائم دائما يكون الهدف منها الكسب المادى، بينما(28.3%) من الشباب عينة الدراسة موزعة بنسبة (22.0%) للذكور فى مقابل (34.5%) للإناث لا يعرفون أكثر الفئات تعرضا لمخاطر الجريمة الإلكترونية. بينما(15.5%) من الشباب عينة الدراسة موزعة بنسبة (17.5%) للذكور فى مقابل (13.5%) للإناث يرون أن أكثر الفئات تعرضا لمخاطر الجريمة الإلكترونية الأفراد ذات المستوى الاجتماعى الاقتصادى المتوسط، بينما(12.0%) من الشباب عينة الدراسة موزعة بنسبة (9.5%) للذكور فى مقابل (14.5%) للإناث يرون أن أكثر الفئات تعرضا لمخاطر الجريمة الإلكترونية الأفراد ذات المستوى الاجتماعى الاقتصادى المنخفض.

تأسيساً على ما سبق يتضح بأنه يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب عينة الدراسة حول أضرار الجريمة الإلكترونية.

جدول رقم (28)

أى الفئات العمرية اكثر تعرضا لمخاطر الجريمة الإلكترونية

العينة	ذكور		إناث		الإجمالي		قيمة z	مدى الدلالة
	ك	%	ك	%	ك	%		
الأطفال	21	10.5	17	8.5	38	9.5	.681	غير دالة
الشباب	124	62.0	146	73.0	270	67.5	2.346	دالة**
الشباب	138	69.0	139	69.5	277	69.3	.108	غير دالة
كبار السن	47	23.5	38	19.0	85	21.3	1.099	غير دالة
جملة من سئلوا	**200**		**200**		**400**			

أوضحت بيانات الجدول السابق أكثر الفئات العمرية تعرضا للجريمة الإلكترونية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاءت فى مقدمة **الفئات العمرية ارتكابا للجريمة الإلكترونية الشباب** بنسبة بلغت (69.3%)، موزعة بنسبة (69.0%) للذكور فى مقابل (69.5%) للإناث. بينما جاء فى الترتيب الثانى من**الفئات العمرية الأكثر تعرضا للجريمة** الإلكترونية الشباب بنسبة بلغت (67.5%)، موزعة بنسبة (62.0%) للذكور فى مقابل (73.0%) للإناث، بينما جاء فى الترتيب الثالث من**الفئات العمرية الأكثر تعرضا للجريمة الإلكترونية كبار السن** بنسبة بلغت (21.3%)، موزعة بنسبة (23.5%) للذكور فى مقابل (19.0%) للإناث، بينما جاء فى الترتيب الرابع من**الفئات العمرية الأكثر تعرضا للجريمة الإلكترونية الأطفال** بنسبة بلغت (9.5%)، موزعة بنسبة (10.5%) للذكور فى مقابل (8.5%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحصائيا بين الذكور والإناث حول أكثر الفئات العمرية تعرضا للجريمة الإلكترونية على النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن أكثر الفئات العمرية تعرضا للجريمة الإلكترونية الشباب** بنسبة بلغت (62.0%)، (73.0%) للإناث على

الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (2.346) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (99%) وقد يرجع ذلك إلى استخدام الشباب للإنترنت هذا مع صغر سنهم وقلة خبرتهم قد يخلق مناخا خصبا لكى يصبحوا من أكثر الفئات تعرضا للجريمة الإلكترونية.

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث حول أكثر الفئات العمرية تعرضا للجريمة الإلكترونية على النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن أكثر الفئات العمرية تعرضا للجريمة الإلكترونية الشباب** بنسبة بلغت (69.0%)، (69.5%) على الترتيب.والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (108.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).
- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن أكثر الفئات العمرية تعرضا للجريمة الإلكترونية كبار السن** (23.5%)، (19.0%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.099) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن أكثر الفئات العمرية تعرضا للجريمة الإلكترونية الأطفال**(10.5%)، (8.5%). على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (681.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

تأسيساً على ما سبق يتضح أن اكثر الفئات ارتكابا للجريمة الإلكترونية من الشباب.

جدول (29)

أراء الشباب حول أكثر ضحايا الجرائم الإلكترونية

النوع الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
الذكور	44	22.0	35	17.5	79	19.8
الإناث	76	38.0	99	49.5	175	43.8
الإثنين على السواء	26	13.0	24	12.0	50	12.5
لا أعرف	54	27.0	42	21.0	96	24.0
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =5.628 درجة الحرية = 3 - مستوى المعنوية=131. غيردالة

تدل بيانات الجدول السابق على:

أن(43.8%) من الشباب عينة الدراسة موزعة بنسبة (38.0%) للذكور فى مقابل (49.5%) للإناث يرون أن أكثر ضحايا الجرائم الإلكترونية من الإناث وقد يرجع ذلك إلى طبيعة الإناث فى أن البعض منهم ليس لديه المهارة الكافية للتعامل العالى مع تقنيات الحاسب كبعض الذكور، بينما أن(24.0%) من الشباب عينة الدراسة موزعة بنسبة (27.0%) للذكور فى مقابل (21.5%) للإناث لايعرفون إلى أى فئة ينتمى ضحايا الجرائم الإلكترونية، فى حين أن (19.8%) من الشباب عينة الدراسة موزعة بنسبة (22.0%) للذكور فى مقابل (17.5%) للإناث يرون أن أكثر ضحايا الجرائم الإلكترونية من الذكور، فى الوقت الذى يرى فيه(12.5%) من الشباب عينة الدراسة موزعة بنسبة (13.0%) للذكور فى مقابل (12.5%) للإناث يرون أن أكثر ضحايا الجرائم الإلكترونية من الاثنين معا.

تأسيساً على ما سبق يتضح أنه لا يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب عينة الدراسة حول أكثر الفئات من ضحايا الجرائم الإلكترونية

جدول (30)

أراء الشباب حول مخاطر الجريمة الإلكترونية تقتصر على الأفراد فقط

النوع / الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	165	82.5	172	86.0	337	84.3
أحياناً	27	13.5	19	9.5	46	11.5
نعم	8	4.0	9	4.5	17	4.3
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =1.596 **درجة الحرية = 2** **مستوى المعنوية=450. غيردالة**

تدل بيانات الجدول السابق على:

أن(84.3%) من الشباب عينة الدراسة موزعة بنسبة (82.5%) للذكور فى مقابل (86.0%) للإناث يرون أن الجريمة الإلكترونية لاتقتصر مخاطرها على الأفراد فقط وهذا قد يعكس معرفة الشباب عينة الدراسة ان الجريمة الإلكترونية لها ضحايا أخرين غير الأفراد، بينما (11.5%) من الشباب عينة الدراسة موزعة بنسبة (13.5%) للذكور فى مقابل (9.5%) للإناث.

يرون أن الجريمة الإلكترونية أحيانا ما تقتصر مخاطرها على الأفراد فقط،بينما (4.3%) من الشباب عينة الدراسة موزعة بنسبة (4.0%) للذكور فى مقابل (4.5%) للإناث يرون أن الجريمة الإلكترونية تقتصر مخاطرها على الأفراد فقط.

تأسيساً على ما سبق يتضح أنه لا يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب عينة الدراسة حول اقتصار مخاطر الجريمة الإلكترونية على الأفراد فقط.

جدول رقم (31)

الجهات الأخرى التى تتعرض لمخاطر الجريمة الإلكترونية

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
المؤسسات	91	55.2	76	44.2	167	49.6	2.010	.044 دالة*
الهيئات	60	36.4	48	27.9	108	32.0	1.661	.019دالة**
الدول	103	62.4	106	61.6	209	62.0	.150	غير دالة
أخرى	20	12.0	23	13.4	43	12.8	.344	غير دالة
جملة من سئلوا	**165**		**172**		**337**			

أوضحت بيانات الجدول السابق أن الجهات الأخرى التى تتعرض لمخاطر الجريمة الإلكترونية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاءت الدول فى مقدمة **الجهات الأخرى التى تتعرض لمخاطر الجريمة الإلكترونية** بنسبة بلغت (62.0%)، موزعة بنسبة (62.4%) للذكور فى مقابل (61.6%) للإناث وقد يعكس ذلك معرفة الشباب بالجريمة الإلكترونية وأنها عابرة الحدود لدرجة انها تصل مخاطرها إلى دول بأكملها. بينما جاء فى الترتيب الثانى المؤسسات بنسبة بلغت (49.6%)، موزعة بنسبة (55.2%) للذكور فى مقابل (44.2%) للإناث وقد يعكس ذلك وعى الشباب بالجريمة الإلكترونية وحجم الأضرار التى تسببها هذه الجريمة. بينما جاء فى الترتيب الثالث الهيئات بنسبة بلغت (32.0%)، موزعة بنسبة (36.4%) للذكور فى مقابل (27.9%) للإناث. بينما جاء فى الترتيب الرابع جهات أخرى غير المذكورة بالجدول بنسبة بلغت (12.8%)، موزعة بنسبة (12.1%) للذكور فى مقابل (13.4%) للإناث.

كما أوضحت النتائج التفصيلية وجود فروق دالة إحصائيا بين الذكور والإناث في الجهات الأخرى التى تتعرض لمخاطر الجريمة الإلكترونية على النحو الأتى:

- تزداد نسبة الذكور الذين يرون **أن المؤسسات من الجهات التى تتعرض لمخاطر الجريمة الإلكترونية عن الإناث** بنسبة بلغت (55.2%)، (44.2%) على الترتيب وقد يعكس ذلك وعى الشباب بخطورة الجريمة الإلكترونية.

- كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث في مصادر معرفة الشباب بوجود جرائم إلكترونية فى مصر على النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن الدول من الجهات التى تتعرض لمخاطر الجريمة الإلكترونية** بنسبة (62.4%)، (61.6%) على الترتيب.
- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن هناك جهات أخرى غير الموجودة بالجدول تتعرض لمخاطر الجريمة الإلكترونية** بنسبة (12.1%)، (13.4%) على الترتيب.

تأسيساً على ما سبق يتضح تعدد الجهات التى تتعرض لمخاطر الجريمة الإلكترونية فهى ليست قاصرة على الأفراد فقط ومعرفة الشباب بهذه الجهات.

جدول (32)

أراء الشباب حول إمكانية مكافحة الجريمة الإلكترونية

النوع الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا	11	5.5	16	8.0	27	6.8
أحياناً	24	12.0	21	10.5	45	11.3
نعم	165	82.0	163	81.5	328	82.0
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =1.138   درجة الحرية = 2   مستوى المعنوية=566. غيردالة

تدل بيانات الجدول السابق على:

أن (82.0%) من الشباب عينة الدراسة موزعة بنسبة (82.0%) للذكور فى مقابل (81.5%) للإناث يرون أنه من الممكن مكافحة الجريمة الإلكترونية وهذه النتيجة قد تشير إلى وعى الشباب عينة الدراسة بأن الجريمة الإلكترونية كغيرها من الجرائم يمكن التصدى لها ومواجهتها، فى حين أن (11.3%) من الشباب عينة الدراسة موزعة بنسبة (12.0%) للذكور فى مقابل (10.5%) للإناث يرون أنه أحيانا يمكن مكافحة الجريمة الإلكترونية،بينما (6.8%) من الشباب عينة الدراسة موزعة بنسبة (5.5%) للذكور فى مقابل (8.0%) للإناث يرون أنه لا يمكن مكافحة الجريمة الإلكترونية هذه النتيجة قد تعكس الفهم العميق من قبل المراهقن عينة الدراسة للجريمة الإلكترونية فعلى الرغم من إمكانية مكافحتها إلا أن هذا الأمر ليس سهلا فالجريمة الإلكترونية من الجرائم التى يصعب إثباتها وتعقبها.

تأسيساً على ما سبق يتضح أنه لا يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب عينة الدراسة حول إمكانية مكافحة الجريمة الإلكترونية.

جدول رقم (33)
سبل مكافحة الجريمة الإلكترونية

العينة	ذكور		إناث		الإجمالي		قيمةz	مدى الدلالة
	ك	%	ك	%	ك	%		
سن القوانين	125	66.1	122	66.3	247	66.2	.034	**غير دالة**
حملات إعلامية لتوعية الشباب بخطورتها	112	59.3	105	57.1	217	58.2	.429	غير دالة
عدم استخدام الحاسب الألى	24	12.7	22	12.0	46	12.3	.218	غير دالة
استخدام الرقابة على الموقع الشخصى للأفراد والهيئات	56	29.6	68	37.0	124	33.2	1.500	غير دالة
استخدام برامج الانترنت المخصصة بالامان والحماية	101	53.4	109	59.2	210	56.3	1.128	غير دالة
عقد الاتفاقيات الدولية	62	32.8	49	26.6	111	29.8	1.302	غير دالة
أخرى	9	4.8	12	6.5	21	5.6	.736	غير دالة
جملة من سئلوا	**189**		**184**		**373**			

أوضحت بيانات الجدول السابق سبل مكافحة الجريمة الإلكترونية جاءت مرتبه وفقا لما أحرزته من تكرارات على النحو التالى:

جاء **سن القوانين فى مقدمة السبل المتبعة لمكافحة الجريمة الإلكترونية** بنسبة بلغت (66.2%) موزعة بنسبة (66.1%) للذكور فى مقابل (66.3%) للإناث وقد يرجع ذلك إلى اعتياد الشباب عينة الدراسة على أن ردع الجريمة ربما لا يتم إلا بالقانون.بينما جاء فى **الترتيب الثانى حملات إعلامية لتوعية الشباب بخطورتها** بنسبة بلغت (58.2%) موزعة بنسبة (59.3%) للذكور فى مقابل (57.1%)، بينما جاء فى **الترتيب الثالث استخدام برامج الانترنت المخصصة بالامان والحماية** بنسبة بلغت (56.3%) موزعة بنسبة (53.4%) للذكور فى مقابل (59.2%)، بينما جاء فى **الترتيب الرابع استخدام الرقابة على الموقع الشخصى**

للأفراد والهيئات بنسبة بلغت (33.2%) موزعة بنسبة (29.6%) للذكور فى مقابل (37.0%)، بينما جاء فى **الترتيب الخامس عقد الاتفاقيات الدولية** بنسبة بلغت (29.8%) موزعة بنسبة (32.8%) للذكور فى مقابل (26.6%) وقد يعكس ذلك وعى الشباب بأن أحد مخاطر الجريمة الإلكترونية يكمن فى أنها عابرة الحدود وبالتالى فهى تحتاج إلى ردع ينتشر على نطاق دولى لإمكانية السيطرة عليها وردع مرتكبها، بينما جاء فى **الترتيب السادس عدم استخدام الحاسب الألى** بنسبة بلغت (12.3%) موزعة بنسبة (12.7%) للذكور فى مقابل (12.0%)، بينما جاء فى **الترتيب السابع سبل أخرى لمكافحة الجريمة الالكترونية** بنسبة بلغت (5.6%) موزعة بنسبة (4.8%) للذكور فى مقابل (6.5%).

كما أوضحت النتائج التفصيلية عدم وجود فروق دالة إحصائيا بين الذكور والإناث حول سمات مرتكبى الجريمة الإلكترونية على النحو الأتى:

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن سن القوانين فى مقدمة السبل المتبعة لمكافحة الجريمة الإلكترونية** بنسبة بلغت (66.1%)، (66.3%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (034.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن حملات إعلامية لتوعية الشباب بخطورتها أحد السبل المتبعة لمكافحة الجريمة الإلكترونية** بنسبة (59.3%)، (57.1%)على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (429.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن استخدام برامج الانترنت المخصصة بالامان والحماية أحد السبل المتبعة لمكافحة الجريمة الإلكترونية** بنسبة (53.4%)، (59.2%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.128) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن استخدام الرقابة على الموقع الشخصى للأفراد والهيئات أحد السبل المتبعة لمكافحة الجريمة الإلكترونية** بنسبة (29.6%)، (37.0%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.500) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أنعدم استخدام الحاسب الألى أحد السبل المتبعة لمكافحة الجريمة الإلكترونية** بنسبة (12.7%)، (12.0%) على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (218.)وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أنعقد الاتفاقيات الدولية أحد السبل المتبعة لمكافحة الجريمة الإلكترونية** بنسبة (32.8%)، (26.6%). على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (1.302) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

- يتقارب نسبة الشباب الذكور والإناث الذين يرون **أن هناك سبل أخرى متبعة لمكافحة الجريمة الإلكترونية** بنسبة (4.8%)، (6.5%). على الترتيب. والفارق غير دال إحصائيا حيث بلغت قيمة Z المحسوبة (736.) وهى أقل من القيمة الجدولية المنبئة بوجود علاقة فارقة بين النسبتين عند بمستوى ثقة (95%).

جدول (34)

أراء الشباب حول تواجد تعاون دولى مشترك لمكافحة الجريمة الإلكترونية

النوع الرأى	ذكور		إناث		الإجمالي	
	ك	%	ك	%	ك	%
لا أعرف	81	40.5	127	63.5	208	52.0
لا	50	25.0	40	20.0	90	22.5
نعم	69	34.5	33	16.5	102	25.5
جملة من سئلوا	**200**	**100**	**200**	**100**	**400**	**100**

قيمة كا^2 =23.990درجة الحرية = 2 مستوى المعنوية = .000 دالة

تدل بيانات الجدول السابق على:

أن(52.0%) من الشباب عينة الدراسة موزعة بنسبة (40.0%) للذكور فى مقابل (60.0%) للإناث لا يعرفون ما إذا كان هناك **تعاون دولى مشترك لمكافحة الجريمة الإلكترونية، بينما** (25.5 %) من الشباب عينة الدراسة موزعة بنسبة (34.5%) للذكور فى مقابل (16.0%) للإناث يرون أن هناك **تعاون دولى مشترك لمكافحة الجريمة الإلكترونية**، بينما (22.5%) من الشباب عينة الدراسة موزعة بنسبة (25.0%) للذكور فى مقابل (20.0%) للإناث يرون أنه لا يوجد تعاون **دولى مشترك لمكافحة الجريمة الإلكترونية**

مجمل نتائج الجدول تشير إلى عدم معرفة الشباب بوجود تعاون دولى لمكافحة الجريمة وقد يرجع ذلك إلى عدم اهتمام العينة بتتبع الجريمة الإلكترونية.

تأسيساً على ما سبق يتضح أنه يوجد فروق ذات دلالة إحصائية بين النوع فى أراء الشباب عينة الدراسة حول إمكانية تواجد تعاون دولى مشترك لمكافحة الجريمة الإلكترونية

خاتمة الكتاب

نود فى نهاية هذا الكتاب الاشارة إلى أنه من الضرورى أن نستخدم كل ماهو جديد ولكن بحدود، ولا نقلد الأخرين تقليدا أعمى من شأنه أن يقودنا إلى ارتكاب أخطاء قد يصعب علينا تجنبها أو محاولة تجاوزها. فالتكنولوجيا بكل ما أحدثته من ثورة علمية ومعلوماتيه فى مجتمعاتنا إلا أن لها أنياب ومخالب أضرت بنا، وتسببت فى كوارث ضخمة داخل مجتمعاتنا العربية, ولكن العيب ليس فى التكنولوجيا ولكن المشكلة تكمن ففى كيفية استخدامنا لها وكيفية تعاملنا معها ومع الأمور من خلالها، لأن الاستخدام الخاطئ للتكنولوجيا الحديثه هو ما ألقانا فى خضم الجرائم الإلكترونية، وجعل منا فريسة سهلة للإرهاب الذى باتت مواقع الانترنت بيئة حاضنة له يستطيع الإرهابيون من خلالها تجنيد الشباب والتشكيك فى معتقداتهم الدينية وتدريبهم على ارتكاب العنف ونشر الفكر المتطرف بالقوة وبالإجبار. وتلقى الأموار والتعليمات من خلالها مما جعل من الارهاب شبحا يهدد بقاء مجتمعاتنا. لذا وجب علينا توعية شبابنا من خطورة الاستعمال غير المحسوب للإنترنت وهذا دور الأسرة والمدرسة والجامعة والمسجد والكنيسة وأخيرا وسائل الإعلام التى لا نستطيع إعفاءها من المسؤلية فى هذا الشأن.

المراجع والمصادر

أولاً: الكتب

1- أمير فرج يوسف: "**الجرائم المعلوماتية على شبكة الإنترنت**"، (الأسكندرية: دار المطبوعات الجامعية، 2008)ص.

2- السيد عتيق: "**جرائم الإنترنت**"، (القاهرة: دار النهضة العربية،2000) ص32.

3- خالد بن سليمان الغثر، محمد بن إبراهيم السويل: "**أمن المعاومات بلغة ميسرة**"،(الرياض: ب.د2009)ص25، 24.

4- طاهر داود: "**جرائم نظم المعلومات**"، (الرياض: ب د 2000)ص.38

5- عمرو عيسى الفقى: "**الجرائم المعلوماتية وجرائم الحاسب الألى والإنترنت فى مصر والدول العربية**"،(القاهرة: المكتب الجامعى الحديث، ب ت)ص97،96.

6- نائلة عادل محمد فريد قورة: "**جرائم الحاسب الاقتصادية**"، مرجع سابق ص.32،31

7- جون كيريللو: "**موسوعة الهاكرز**"، ط 2(القاهرة: دار الفاروق للنشر والتوزيع،2007) ص .600،59

8- ريتشارد مانسفيلد، ترجمة خالد العامرى: "**حيل وأساليب الهاكرز وطرق الوقاية منها**"، ط2 (القاهرة: دار الفاروق للنشر والتوزيع، 2006) ص32،31.

9- محمد حسام محمود لطفى: "**الحماية القانونية لبرامج الحاسب الإلكترونى**"، (القاهرة: دار الثقافة للطباعة والنشر،1987)ص.7

10- أحمد خليفة الملط: "**الجرائم المعلوماتية**"، مرجع سابق ص .181

11- حسن طاهر داود: "**الحاسب وأمن المعلومات**"، (الرياض: ب.د،2000) ص65.

12- شمس الدين إبراهيم: "**وسائل مواجهة الإعتداء على الحياة الشخصية فى مجال تقنية المعلومات فى القانون السودانى**"، (القاهرة: دار النهضة العربية، 2005) ص.79

13- جميل عبد الباقى الصغير: "**القانون الجنائى والتكنولوجيا الحديثة: الكتاب الأول الجرائم الناشئة عن استخدام الحاسب الألى**"، ط1 (القاهرة: دار النهضة العربية،1992) ص.49،48

14- محمد شلال العانى:" **التشريع الجنائى الإسلامى**"، ط2 (الأردن: مؤسسة المروة للطباعة،1993) ص.165

15- نهاد كريدى: "**الجريمة والاحتيال فى البيئة الإلكترونية**"، (بيروت: ب د،2008) ص 16،14.

16- حسنى عبد السميع ابراهيم: "**الجرائم المستحدثة على الانترنت**"، (القاهرة: دار النهضة العربية ،2011) ص 254،252.

17- عزة على محمد الحسن: "**الجريمة المعلوماتية فى القانون السودانى**" ص.104،105

18- محمد حسام محمود لطفى:"**المرجع العلمى فى الملكية الأدبية والفنية فى ضوء أراء الفكر وأحكام القضاء**"، ط1 (القاهرة: ب د،1992)ص.197

19- عمر بن يونس، يوسف أمين: "**غسل الأموال عبر الانترنت**"، ط1 (القاهرة : ب د،2004)ص31.

20- عمر بن يونس: "**المخدرات والمؤثرات العقلية عبر الإنترنت**"، (الأسكندرية: دار الفكر الجامعى، 2004) ص46.

21- على حبار االحسيناوى: "**جرائم الحاسوب والإنترنت**"،(عمان: دار اليازورنى،2009) ص.93

22- سامى على حامد عياد: "**الجريمة المعلوماتية واجرام الإنترنت**"، (الأسكندرية: دار الفكر الجامعى،2007) ص.91

23 - هلالى عبد الله أحمد: "**التزام الشاهد بالإعلام فى الجرائم المعلوماتية**"، ط 1 (القاهرة: دار النهضة العربية،1997) ص.21

24- جميل عبد الباقى الصغير: "**الإنترنت والقانون الجنائى**"، (القاهرة: دار النهضة العربية،2001) ص41.

25- محمد فتحى: "**الإنترنت شبكة العجائب**"، (القاهرة: دار اللطائف، 2003) ص69-71.

26- محمد صلاح سالم: "**العصر الرقمى وثورة تكنولوجيا المعلومات**" ط1، (القاهرة: عين للدراسات والبحوث الانسانية والاجتماعية،2002) ص182.

27- نبيلة هبة هروال: "**الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الإستدلالات**"، (القاهرة: دار الفكر الجامعى،2007) ص.35

28- نائلة محمد فريد قورة: "**جرائم الحاسب الإقتصادية**"، دراسة نظرية وتطبيقية،(القاهرة: دار النهضة العربية، 2004)ص.47

29- منير محمد الجهينى، ممدوح محمد الجهينى: **جرائم الإنترنت والحاسب الألى ووسائل مكافحتها**"، القاهرة: دار الفكر الجامعى،2004)ص16.

30- هشام محمد فريد رستم: "**قانون العقوبات ومخاطر تقنية المعلومات**"، (أسيوط: مكتبة الألات الحديثة،1994) ص42،41.

31- محمد عبيد الكعبى: "**الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت**"،ط2 (القاهرة: دار النهضة العربية،2009)ص38.

32- محمد عبد الرحيم سلطان: "جرائم الإنترنت والإحتساب عليها"، **مؤتمر القانون والكمبيوتر والإنترنت** (العين: جامعة الإمارات، مايو 2002).

33- أحمد خليفة الملط: **"الجرائم المعلوماتية: دراسة مقارنة"**، ط1 (القاهرة: دار الفكر الجامعى،2006) ص.95

34- خالد محمد كدفور المهيرى:**"جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية"**، (دبى: دار العزيز للطباعة والنشر، 2005) ص118.

35- خالد ممدوح إبراهيم: **"أمن الجريمة الإلكترونية"**، (الدار الجامعية، 2010)ص.55

36- عبد الفتاح بيومى حجازى: **"مبادىء الإجراءات القانونية فى جرائم الكمبيوتر والإنترنت"**، ط1 (القاهرة: دار الفكر العربى،2006) ص45- 46.

37- أيمن عبد الحفيظ: "الإتجاهات الأمنية والفنية لمواجهة الجرائم المعلوماتية"، (القاهرة: ب.د، 2005)ص13،14.

38- أحمد ضياء: **"الظاهرة الإجرامية بين الفهم والتحليل"**، (القاهرة: دار النهضة العربية، 2001)ص 294- .295

39- رمسيس بهنام: **"المجرم تكوينا وعقيدة"**، (الأسكندرية: منشأة دار المعارف، ب ت) ص176،177.

40- عمر محمد أبوبكر بن يونس: **"الجرائم الناشئة عن استخدام الإنترنت الجوانب الموضوعية والإجرائية"**، (القاهرة: دار النهضة العربية، 2004) ص.140،141.

41- محمد سامى الشوا: **"ثورة المعلومات وانعكاستها على قانون العقوبات"**، (القاهرة: دار النهضة العربية، 1994) ص.7

42- انتصار أنور الغريب: **"أمن الكمبيوتر والقانون"**، (بيروت: دار الراتب الجامعية، 1994) ص10.

43- رمسيس بهنام: **"المجرم تكوينا وعقيدة"**، (الأسكندرية: منشأة دار المعارف، ب ت) ص175.

44- عبد الفتاح بيومى حجازى: **مكافحة جرائم الكمبيوتر والإنترنت فى القانوت العربى النموذجى"**، ط1 (القاهرة: دار الفكر العربى، 2006)ص.89

45- عبد الله حسين على محمود: **"سرقة المعلومات المخزنة فى الحاسب الألى"**، ط1 (القاهرة: دار النهضة العربية،2001)ص.79،80

46- محمد على العريان: **"الجرائم المعلوماتية"**، (الأسكندرية: دار الجامعة الجديدة للنشر، 2004) ص.67،68

47- بهاء شاهين: **"الإنترنت والعولمة"**، ط1 (القاهرة: عالم الكتب، 1999) ص.59

48- محمد حماد الهيتى: "**جرائم الحاسوب**"، ط1 (عمان: دار المناهج، 2006) ص163.

49- محمود أبو عباينة: "**جرائم الحاسوب وأبعادها الدولية**"، (عمان: دار الثقافة،2005) ص.152

50- حمد أمين أحمد: "**جرائم الحاسوب والإنترنت – الجريمة المعلوماتية**"، (عمان: دار الثقافة، 2004) ص.74

51- حسام ملحم، عمار خير بك: "**شبكات الانترنت بنيتها الأساسية وانعكاساتها على المؤسسات**"، ط1(دار الرضا، 2000) ص 118.

52- زياد القاضى، قضى القاضى وأخرون: "**مقدمة إلى الانترنت**"، ط1 (عمان: دار صفاء للنشر والتوزيع، 2000) ص213-.216

53- مخلد خلف النوافعة: "**اتجاهات الجمهور الأردنى إزاء قضايا الإرهاب التى تبثها قناتا الجزيرة والعربية الفضائيتان الإخباريتان**" (جامعة الشرق الأوسط: كلية الإعلام، 2010) ص.64

54- أمير أفونس عريان: "**الجرائم الإلكترونية فى البنوك وكيفية مواجهتها**" (جامعة عين شمس: كلية التجارة، 2010) ص4.

55- يحي على دماس: "**دور تقنيات التواصل الاجتماعى فى التوعية بالعمليات الارهابية**" (جامعة نايف العربية للعلوم الأمنية، 2013) ص31.

ثانياً: رسائل الماجستير والدكتوراه.

1- محمد على العريان: "**الجرائم المعلوماتية**"، ط1 (الأسكندرية: دار الجامعة الجديدة، 2004) ص66.

2- منى فتحى أحمد عبد الكريم: "الجريمة عبر الشبكة الدوليه صورها ومشاكل اثباتها"، **رسالة دكتوراه غير منشورة** (جامعة القاهرة: كلية الحقوق، 2007) ص 28،29.

3- أحمد حسام طه تمام: "الجرائم الناشئة عن استخدام الحاسب، الحماية الجنائية للحاسب الألى"، **رسالة دكتوراه غير منشورة** (جامعة طنطا: كلية الحقوق، 2000) ص.210،211.

4- أيمن عبد الحفيظ عبد الحليم سليمان: "استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الألى"، **رسالة دكتوراه غير منشورة** (أكاديمية الشرطة، 2004)ص49.

5- مديحة فخرى محمود محمد: "دور الجامعات المصرية فى مواجهة الجرائم الإلكترونية"، **رسالة دكتوراه غير منشورة** (جامعة حلوان: كلية التربية،2011) ص10.

6- أيمن عبد الله فكرى: "جرائم نظم المعلومات"، **رسالة دكتوراه غير منشورة**،(جامعة المنصورة: كلية الحقوق، 2006)ص81.

ثالثاً: بحوث علمية منشورة.

1- أحمد الطاهر النور: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية - الجرائم الإلكترونية غير الوطنية، بحث مقدم للندوة القانونية المتخصصة، الخرطوم 6،5 مارس 2000، ص12.

2- غنام محمد غنام: "عدم ملاءمة القواعد التقليدية فى قانون العقوبات لمكافحة جرائم الكمبيوتر"، مؤتمر القنون والكمبيوتر والإنترنت جامعة الإمارات: كلية الشريعة والقانون، 2000) ص1.

3- يونس عزب: "جرائم الكمبيوتر والإنترنت" (أبوظبى: المركز العربى للدراسات والبحوث الجنائية) مؤتمر الأمن العربى ص19،20.

4- سعد عطوة الزنط: الارهاب الالكترونى واعادة صياغة استراتيجيات الأمن القومى، مؤتمر الجرائم المستحدثة كيفية اثباتها ومواجهتها (المركز القومى للبحوث الاجتماعية والجنائية،2010).

5- رولا الحمصى: ادمان الانترنت عند الشباب وعلاقته بمهارات التواصل الاجتماعى دراسة ميدانية، مؤتمر ماتقى الطلاب الإبداعى الثانى عشر، جامعة أسيوط.

6- عبد الله بن عبدالعزيز بن فهد العجلان: بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت", والمنعقد بالقاهرة في المدة من 2 - 4 يونيو 2008م 30.

7- أحمد على البدرى: الإرهاب الإلكترونى، ورقة عمل المؤتمر الثانى للمركز القومى للبحوث الاجتماعية والجنائية - الجرائم المستحدثة كيفية إثباتها ومواجهتها فى الفترة من 15- 16 ديسمبر 2016، ص8-9.

8- فايز الشهري: التطرف الالكترونى على شبكة الانترنت رؤية تحليلية، مؤتمر تقنية المعلومات والأمن الوطنى،12-14 /2008/11.

9- عطا الله بن فهد السرححانى: توظيف شبكات التواصل الاجتماعى فى مكافحة الارهاب، دورة تدريبية خلال الفترم من 23-27 /2013/2م.

10- جوان فؤاد معصوم: بحث الارهاب الالكترونى، ورشة عمل بعنوان (مكافحة الارهاب ضرورة وطنية) ولفترة يومين 15 - 16 تشرين 2016 العراق.

11- السيد عوض: التطور التكنولوجى. والجريمة، المؤتمر السنوى الرابع والثلاثون قضايا السكان والتنمية، 19 - 23 ديسمبر 2004، ص11.

12- على حسنى عباس: الاستخدام الأمن لشبكة الإنترنت وطرق الوقاية من مخاطر استخدامها، ورقة عمل، 2010، ص5.

13- إبراهيم محمد جاسم: المواجهة العلمية فى مواجهة الارهاب فى الشبكات الاجتماعية، دورة تدريبية فى الفترة من 23-2013/2/27م، ص 10.

14- رائد العدوان: المعالجة الدواية لقضايا الإرهاب الإلكترونى، دورة تدريبية فى الفترة من 23-2003/2/27، ص9 – 10.

15- رامى متولى: الجرائم المعلوماتية وطرق مواجهتها، ورقة عمل مؤتمر تأمين المعلومات والدليل الرقمى وكيفية إثباته فى الجرائم الإلكترونية (15 - 16 ديسمبر 2010) المركز القومى للبحوث الاجتماعية والجنائية ص.8

16- أحمد محمد أمين الشريف:الجرائم المستحدثة عبر الإنترنت فى مجال حماية الأداب العامة، ورقة عمل الادارة العامة لحماية الأداب، ص.9

17- عارف خليل أبو عيد: "جرائم الإنترنت"، دراسة مقارنة، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 5، العدد 3 أكتوبر .2008

18- محمد أمين الرواس:جرائم الكمبيوتر والانترنت،(الاسكندرية: دار المطبوعات الجامع،2004).

19- David I Cave&William Vastorch:**Computer Crime Acrime Fight** (Reilly&Associate, nc1995) p 61.

رابعاً: المصادر

1- moelalfy@yahoo.com

جرائم الانترنت كأحد الجرائم المستحدثة بتاريخ 30/1/ 2008.

2- http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx-

شيماء عبدالغني محمد عطا الله: "مكافحة جرائم المعلوماتية في المملكة العربية السعودية"، **بحث منشور على الانترنت.**

3- www.Minshawi.com
4- http://forum.biskra7.com
5- www Wikipedia..com
6- www.Knwledge Society,in Wikipedia.org
7- http://sy-street.net
8-http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/forensic-and-computer-crimes/
9- www.lipa-lb.org

10- هنا أبو جريشة الحداد: "الجريمة الإلكترونية فيرس: قرصنه – احتيال" **بحث منشور على الانترنت.**

11- http://www.babylon.com

أحمد سمير : الجريمة المعلوماتية **بحث منشور على الإنترنت.**

12- http://www.arablaw.org/

13- http://www.arablaw.org/

14- www.Minshawi.com

جرائم الإنترنت من منظور شرعى وقانونى، **بحث منشور على الإنترنت** لمحمد المنشاوى.

15- http://www.arablaw.org/Download/CyberCrimes_WorkPaper.doc

بحث حول أدلة الاثبات الحديثة فى القانون، لفراح منانى.

16- http://www.alriyadh.com/2012/03/31/article723214.html
جريدة الرياض الاقتصادى، العدد 15823- الخميس 20/10/2011.

17- http://www.moheet.com
18https://units.imamu.edu.sa/deanships/dialogue_civilizations/news/Pages/erhab-5.aspx
100- www.shaimaattalla.com

19- **تايم لاين جريدة الرياض**، العدد 17202، الخميس 14 شوال 1436 هـ - 30 يوليو 2015م.

20- http://www.alhayat.com/Articles/

21- محمود علم الدين: وسائل التواصل الاجتماعى والأمن القومى وكيف واجهت الدول مخاطر الانترنت والفيسبوك، **جريدة أخبار اليوم**، العدد 3749، 10 سبتمبر 2016.

22- http://iipdigital.usembassy.gov/st/arabic/publication/2008
23- http://www.alarab.co.uk/?id=

24- رضوى عمار: دور الإعلام فى انتشار ظاهرة الإرهاب، **مجلة السياسة الدولية**،2016/9/1.

25- http://www.assakina.com/book/45994.html

الإرهاب والجريمة الالكترونية بالمجتمع السعودي.

26- http://www.rcssmideast.org/Article/

رؤى المراكز البحثية الغربية للإرهاب في الشرق الأوسط.

27- فايز الشهرى: التطرف الالكترونى سمة المجتمعات عصر العولمة، **جريدة الرياض**، العدد14411، 8ديسمبر 2007.

28- فايز الشهرى: الوجه التقنى للعنف: الانترنت نموذجا، **جريدة الرياض**، العدد13327، 19ديسمبر 2004.

29- فايز الشهرى: ثقافة التطرف والعنف على شبكة الانترنت الاتجاهات والملامح، **مركز الدراسات والبحوث**، 2012.

30- لمياء محسن محمد حسن:شبكات التواصل الاجتماعية العربية والعالمية، **مجلة الاذاعة والتليفزيون**، العدد الأول - يناير - مارس 2015، ص378.

31- **جريدة الرأى**، العدد13585، السبت 10 سبتمبر 2016.

32- http://iipdigital.usembassy.gov/st/arabic/publication/2008

33- فايز الشهرانى: الأنترنت سلاح الإرهاب الجديد، **جريدة الرياض**- العدد 16985،25 ديسمبر 2014م.

34- الارهب الالكترونى والشبكة العنكبوتية بتاريخ 2014/12/24.

35- فايز الشهرى: الوجه التقنى للعنف، الانترنت نموذجا، **جريدة الرياض –** العدد13327،2004.

36- نصيرة تامى: **دور الإعلام الفضائي في التصدي لظاهرة الإرهاب: الإعلام الفضائي العربي نموذجا.**

http://temmaryoucef.ab.ma/144191.htm

37- الاعلام والارهاب: استراتيجية المواجهة، **شبكة الأخبار العربية**، 10 سبتمبر 2016.

38- http://www.alhayat.com

39- http://www.assakina.com/book/71701.htm

40- محمود علم الدين**:** وسائل التواصل الاجتماعي والأمن القومي: **جريدة أخبار اليوم**، العدد 3749، 10 سبتمبر 2015.

41- جريدة الرأى: العدد 13585، السبت 10 سبتمبر 2016.

42- السيد ياسين: **المركز العربى للبحوث والدراسات**، 10 سبتمبر 2016م.

43- فايز الشهوي: الانترنت سلاح الارهاب الجديد، **جريدة الرياض –** العدد25،16985 ديسمبر .2014

44- **جريدة الرأى**، العدد 13585 السبت 10 سبتمبر 2016.

45- https://seconf.wordpress.com/

فهـرس المحتويـات

فهرس الجداول

د. غادة نصار

المؤهلات العلمية والوظيفة:

- ليسانس الأداب بتقدير جيد – كلية الأداب قسم الإعلام – جامعة بنها 2004.
- ماجستير فى دراسات الطفولة – جامعة عين شمس بتقدير ممتاز 2009.
- دكتوراة الفلسفة فى دراسات الاعلام – جامعة عين شمس 2013.
- شهادة الرخصة الدولية لقيادة الكمبيوتر (ICDL) 2012.
- مدرس بقسم الاذاعة والتليفزيون – المعهد الدولى العالى للإعلام – أكاديمية الشروق.

الدورات التى حصلت عليها:

- "توصيف المقررات وخرائط المنهج"، الهيئة القومية لضمان جودة التعليم 2015.
- "التخطيط الاستراتيجى لمؤسسات التعليم العالى"، الهيئة القومية لضمان جودة التعليم 2015.
- "استخدام التكنولوجيا فى التدريس"، مركز تنمية قدرات أعضاء هيئة التدريس، جامعة عين شمس 2013.
- "مهارات الاتصال"، مركز تنمية قدرات أعضاء هيئة التدريس ، جامعة عين شمس 2013.
- "التويفيل"، مركز الخدمة العامة، جامعة عين شمس عام 2008.

المؤتمرات العلمية المشاركة فيها:

- مؤتمر "نحو حياة أفضل للجميع" 2012 والحصول على شهادة تقدير للمشاركة الفعالة بالمؤتمر من معهد الدراسات العليا للطفولة- جامعة عين شمس.
- مؤتمر "الانترنت كوسيلة اعلامية والمخاطر الصحية الناجمة عنه"- جامعة عين شمس.
- مؤتمر "الاعلام وثقافة العنف" – كلية الاعلام – جامعة القاهرة 2016.

مؤلفات تحت الطبع:

- الجريمة الإلكترونية والارهاب.
- وسائل الاعلام وثقافة الحوار.
- دليل الاعلام الجديد.
- دليل القنوات الاخبارية ووكالات الأنباء.

للتواصل: ahmed20007712@yahoo.com